Cambium PTP 800 Series User Guide

System Release 800-05-02

Cambium Networks

Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Components, units, or 3rd Party products used in the product described herein are NOT fault-tolerant and are NOT designed, manufactured, or intended for use as on-line control equipment in the following hazardous environments requiring fail-safe controls: the operation of Nuclear Facilities, Aircraft Navigation or Aircraft Communication Systems, Air Traffic Control, Life Support, or Weapons Systems (High Risk Activities). Cambium and its supplier(s) specifically disclaim any expressed or implied warranty of fitness for such High Risk Activities.

© 2012 Cambium Networks Limited. All Rights Reserved.

Important safety information

This section describes important safety guidelines that must be observed by personnel installing or operating PTP 800 equipment.

⚠ WARNING

To prevent loss of life or physical injury, observe the safety guidelines in this section.

Power lines

Exercise extreme care when working near power lines.

Working at heights

Exercise extreme care when working at heights.

Grounding and protective earth

The outdoor unit (ODU) and compact modem unit (CMU) for the PTP 800 must be properly grounded. It is the user's responsibility to install the equipment in accordance with national regulations. In the USA, follow Section 810 of the *National Electric Code, ANSI/NFPA No.70-1984* (USA). In Canada, follow Section 54 of the *Canadian Electrical Code*. These codes describe correct installation procedures for grounding the ODU, CMU, mast, lead-in wire and discharge unit, size of grounding conductors and connection requirements for grounding electrodes. Other regulations may apply in different countries and therefore it is recommended that installation of the outdoor unit be contracted to a professional installer.

The PTP 800 ODU and CMU must be grounded to a protective earth in accordance with the Local Electrical Regulations.

Electrical safety

The power cable connections must meet International Electrotechnical Commission (IEC) safety standards.

Always power down and unplug the equipment before servicing.

When using alternative DC supplies, such as battery-backed DC power source, the supply must be SELV rated.

Primary disconnect device

The power supply must include a primary disconnect device with appropriate fusing.

External cables

Safety may be compromised if outdoor rated cables are not used for connections that will be exposed to the weather.

RF exposure near the antenna

Strong radio frequency (RF) fields will be present close to the antenna when the transmitter is on. Always mute the transmitter before undertaking maintenance activities in front of the antenna.

Ensure that people cannot stand or walk in front of the antenna within ± 10 degrees of the antenna axis and within the minimum distances listed in Table 210 (ETSI) or Table 211 (FCC). The minimum distances in these tables have been calculated using worst-case assumptions. Reduced separation distances may be appropriate under some circumstances. Further details are provided in Radiation hazard assessment on page 4-86.

Thermal safety

The CMU may be hot to the touch when in operation. The CMU must not be operated in ambient temperatures exceeding 40 deg C unless mounted in a Restricted Access Location. For more information, see Maximum operating ambient temperature for the CMU on page 5-77.

Contents

Important safety information I
About This User Guide 1
General information 2
Version information 2
Contacting Cambium Networks 2
Problems and warranty 4
Security advice 6
Warnings, cautions, and notes 7
Caring for the environment 8
Licensing requirements 9
Operating license 9
Cambium license agreement 9
Chapter 1: Product description 1-1
Overview 1-2
Key features 1-2
Supported bands and frequencies 1-3
Typical users and applications 1-4
System components 1-5
Link types 1-6
Compact modem unit (CMU) 1-8
CMU description 1-8
CMU interfaces 1-9
Further reading on the CMU 1-12
Outdoor unit (ODU) 1-13
ODU description 1-13
ODU interfaces 1-14
Further reading on the ODU 1-17
Indoor RF unit (IRFU) 1-18
IRFU description 1-18
Transceivers 1-19
Branching unit 1-19

IRFU availability 1-19
IRFU configuration options 1-20
IRFU interfaces 1-25
Further reading on the IRFU 1-26
Antennas and couplers 1-27
Antennas 1-27
Remote mounting kits (RMKs) 1-29
Coupler mounting kits 1-30
Direct mount dual-polar antennas 1-32
Further reading on antennas and couplers 1-33
Cabling and lightning protection 1-34
Lightning protection (ODU platforms only) 1-34
RFU to CMU connections 1-34
CMU to network connections 1-34
Cable grounding (ODU platforms only) 1-34
Further reading on cabling and lightning protection 1-36
Wireless operation 1-37
Channel separation 1-37
Channel bandwidth 1-37
Modulation modes 1-38
Adaptive coding and modulation 1-38
Automatic transmitter power control 1-38
Maximum receive power 1-39
Maximum transmit power 1-40
Security 1-40
Further reading on wireless operation 1-40
Ethernet bridging 1-42
Customer network 1-42
Management network 1-43
Protocol model 1-46
Further reading on Ethernet bridging 1-50
System management 1-51
Management agent 1-51
Web server 1-51
Installation wizard 1-53
Configuration pages 1-53
RADIUS authentication 1-53

Email alerts 1-54
SNMP 1-54
Simple Network Time Protocol (SNTP) 1-56
SNMPv3 security 1-56
System logging (syslog) 1-59
AES license 1-60
Login information 1-61
Flexible capacity upgrades 1-61
Software upgrade 1-62
Recovery mode 1-62
Further reading on system management 1-63
1+1 Hot Standby link protection 1-64
1+1 Hot Standby overview 1-64
1+1 Hot Standby link antenna options 1-65
Bridging in 1+1 links 1-66
Receive Diversity 1-67
Further reading on 1+1 Hot Standby 1-69
FIPS 140-2 1-70
FIPS 140-2 capability 1-70
FIPS 140-2 mode 1-71
Further reading on FIPS 140-2 1-72
Chapter 2: Planning considerations 2-1
Link planning 2-2
Process 2-2
Site selection 2-3
Wind loading 2-3
Maximum IF cable length 2-3
Power supply considerations 2-4
PTP LINKPlanner 2-5
Grounding and lightning protection 2-7
The need for power surge protection 2-7
Standards 2-7
Lightning protection zones 2-8
General protection requirements 2-9
Protection requirements for a mast or tower installation 2-11
Protection requirements for the ODU on a high rise building 2-13
Protection requirements for the IRFU 2-17

Data network planning 2-18
Management mode 2-18
VLAN membership 2-19
Priority for management traffic 2-19
IP interface 2-19
Quality of service for bridged Ethernet traffic 2-19
Fast Ethernet port shutdown 2-21
Security planning 2-22
Planning for SNTP operation 2-22
Planning for AES encryption 2-22
Planning for HTTPS/TLS operation 2-23
Planning for FIPS 140-2 operation 2-24
Planning for SNMPv3 operation 2-25
Planning for RADIUS operation 2-28
Planning 1+0 links 2-30
Concept of a 1+0 link 2-30
Antenna, RFU and CMU configurations for 1+0 2-30
Network configurations for 1+0 2-34
Planning 1+1 Hot Standby links 2-35
Concept of a 1+1 Hot Standby link 2-35
Antenna, RFU and CMU configurations for 1+1 2-35
Designating primary and secondary units 2-42
Link Planning for 1+1 Hot Standby links 2-42
Network configurations for 1+1 2-43
Planning for Receive Diversity 2-46
Planning 2+0 links 2-49
Concept of a 2+0 link 2-49
Antenna, RFU and CMU configurations for 2+0 2-49
Network configurations for 2+0 2-55
Frequency spacing in 2+0 ODU based links 2-55
Frequency spacing in 2+0 IRFU based links 2-55
Ordering components 2-57
Ordering CMUs 2-57
Ordering antennas 2-59
Ordering ODUs 2-69
Ordering IF cable, grounding and LPUs 2-80
Ordering RMKs and waveguides 2-85

Ordering coupler mounting kits 2-88
Ordering OMKs 2-90
Ordering IRFUs and accessories 2-91
Ordering network connection components 2-96
Ordering capacity upgrades 2-97
Chapter 3: Legal information 3-1
Cambium Networks end user license agreement 3-2
Acceptance of this agreement 3-2
Definitions 3-2
Grant of license 3-2
Conditions of use 3-3
Title and restrictions 3-4
Confidentiality 3-4
Right to use Cambium's name 3-5
Transfer 3-5
Updates 3-5
Maintenance 3-5
Disclaimer 3-6
Limitation of liability 3-6
U.S. government 3-7
Term of license 3-7
Governing law 3-7
Assignment 3-8
Survival of provisions 3-8
Entire agreement 3-8
Third party software 3-8
Hardware warranty 3-20
Limit of liability 3-21
Chapter 4: Reference information 4-1
Equipment specifications 4-2
CMU specifications 4-2
ODU specifications 4-5
IRFU specifications 4-8
Flexible waveguide specifications 4-10
Coupler mounting kit specifications 4-15
Protection interface specifications 4-17
Wireless specifications 4-19

General wireless specifications 4-19
Frequency bands and channel separation 4-20
Capacity, transmit power and sensitivity 4-22
Data network specifications 4-71
Ethernet interfaces 4-71
Ethernet bridging 4-72
Syslog message formats 4-73
Format of syslog server messages 4-73
Configuration and status messages 4-73
Event messages 4-74
Network management specifications 4-77
Standard SNMP MIBs 4-77
Electromagnetic compliance 4-82
Electrical safety compliance 4-82
EMC immunity compliance 4-82
Compliance testing 4-83
Notifications 4-84
Radiation hazard assessment 4-86
ETSI method 4-86
FCC method 4-88
Chapter 5: Installation 5-1
Preparing for installation 5-2
Safety precautions during installation 5-2
Grounding and lightning protection requirements 5-2
Selecting installation options 5-2
Preparing personnel 5-3
Preparing inventory 5-3
Preparing tools 5-3
Unit pre-configuration 5-4
Installing antennas and ODUs 5-5
Installing a direct mount antenna with one ODU 5-6
Installing a remote mount antenna with one ODU 5-9
Installing a direct mount antenna with two ODUs (via coupler) 5-20
Installing a remote mount antenna with two ODUs (via coupler) 5-26
Installing a direct mount dual-polar antenna with two ODUs 5-33
Installing the IF and ground cables 5-36
Preparing IF cables 5-38

Fitting an N type connector to an IF cable 5-38
Connecting the ODU to the top LPU 5-42
Weatherproofing an N type connector 5-45
Hoisting the main IF cable 5-49
Installing and grounding the main IF cable 5-52
Making an IF cable ground point 5-54
Installing and grounding the IF cable at building entry 5-58
Testing the ODU and IF cable 5-60
Recommended pre-power tests 5-60
Test equipment 5-60
Test preparation 5-61
Testing cable loss 5-62
Measuring distance to fault 5-67
Installing antennas and IRFUs 5-70
Preparation 5-70
Installing the IRFU in the rack 5-71
Connecting the flexible waveguide to the IRFU 5-72
Connecting the CMU cables to the IRFU 5-73
Grounding the IRFU 5-74
Connecting power to the IRFU 5-76
Installing the CMU 5-77
Maximum operating ambient temperature for the CMU 5-77
Operation of CMU in a Restricted Access Location 5-77
Mounting the CMU 5-78
Grounding the CMU 5-80
Connecting the CMU to the IF cable 5-81
Connecting the CMU power supply 5-82
Preparing network connections (1+0 and 2+0 links) 5-84
Installing a copper data interface 5-85
Installing a fiber data interface 5-86
Installing a management interface 5-87
Connecting fiber cables to the CMU 5-88
Preparing network connections (1+1 Hot Standby) 5-89
Installing an out-of-band protection splitter 5-90
Installing a redundant copper interface 5-91
Installing a redundant fiber interface 5-92
Installing a Fiber-Y interface 5-93

Installing a protection cable 5-94
Replacing IRFU components 5-95
Replacing a transceiver 5-97
Replacing a branching unit 5-100
Replacing filters 5-102
Replacing a fan assembly 5-103
Replacing an RF cable 5-104
Chapter 6: Configuration and alignment 6-1
Preparing for configuration and alignment 6-2
Safety precautions during configuration and alignment 6-2
Regulatory compliance during configuration and alignment 6-2
Selecting configuration options 6-2
Task 1: Connecting to the unit 6-3
Configuring the management PC 6-3
Updating the ARP table 6-5
Connecting to the PC and powering up 6-6
Logging into the web interface 6-6
Task 2: Configuring IP and Ethernet interfaces 6-8
Managing the units during configuration and alignment 6-8
Configuring the IP interface and management mode 6-10
Reconnecting to the management PC 6-19
Task 3: Installing license keys 6-21
Checking licensed capabilities 6-21
Generating a new license key 6-23
Entering a new license key 6-23
Starting the full capacity trial 6-24
Task 4: Upgrading software version 6-25
Checking the installed software version 6-25
Upgrading to a new software version 6-26
Task 5: Configuring security 6-28
Configuring AES encryption 6-29
Configuring AES encryption in an operational link 6-31
Configuring HTTPS/TLS 6-32
Using the Security Wizard 6-33
Configuring local user accounts 6-42
Changing own user password 6-48
Protecting access to the summary and status pages 6-49

Configuring RADIUS authentication 6-50
Task 6: Configuring protection 6-53
Configuring unprotected links 6-53
Configuring 1+1 Hot Standby links 6-54
Upgrading an unprotected link to 1+1 Hot Standby 6-61
Task 7: Configuring wireless interface 6-63
Prerequisites for the Installation Wizard 6-63
Starting Installation Wizard 6-63
Step 1: Enter equipment details 6-65
Step 2: Enter details of the radio license 6-69
Step 3: Configuring wireless parameters 6-72
Step 4: Confirming installation configuration 6-73
Step 5: Skipping antenna alignment 6-75
Step 6: Completing configuration without alignment 6-76
Task 8: Setting up SNMP agent 6-77
Configuring SNMPv3 agent 6-77
Configuring SNMPv1/2c agent 6-86
Task 9: Configuring alarms and messages 6-90
Configuring generation of diagnostics alarms 6-90
Configuring generation of email messages 6-92
Task 10: Configuring syslog 6-94
Configuring system logging (syslog) 6-94
Task 11: Configuring remote access 6-96
Configuring web-based management attributes 6-96
Task 12: Aligning antennas 6-98
Introduction to antenna alignment 6-98
Prerequisites for alignment 6-99
Aligning protected antennas 6-99
Aligning dual-polar antennas 6-99
Aligning a pair of antennas 6-100
Step 5: Starting antenna alignment 6-100
Step 6: Aligning antennas 6-100
Step 7: Completing alignment 6-105
Task 13: Reviewing configuration and performance 6-106
Reviewing system configuration attributes 6-106
Comparing actual to predicted performance 6-110
Task 14: Configuring quality of service 6-111

Configuring quality of service 6-111
Task 15: Connecting link to the network 6-114
Connecting to the network 6-114
Setting the real-time clock 6-115
Saving the system configuration 6-119
Configuring for FIPS 140-2 applications 6-121
Prerequisites for FIPS 140-2 configuration 6-121
Configuration procedures for FIPS 140-2 6-122
Checking that the unit is in FIPS 140-2 secure mode 6-122
HTTPS key size warning 6-123
Chapter 7: Operation 7-1
Web-based management 7-2
Accessing the web interface 7-2
Using the menu options 7-4
Viewing the system summary 7-6
Viewing the system status 7-7
Identifying a unit from the web browser title 7-12
Logging out 7-14
Managing alarms and events 7-15
Managing alarms 7-15
Managing email alerts 7-24
Managing SNMP traps 7-24
Managing event notification messages 7-31
Disabling and enabling the wireless interface 7-32
Disabling wireless transmission 7-32
Enabling wireless transmission 7-32
Managing 1+1 Hot Standby links 7-33
Viewing the status of a 1+1 Hot Standby link 7-33
Using the Protected Link page 7-36
Forcing protection switches 7-37
Enabling and disabling fault protection 7-43
Replacing a CMU in a 1+1 Hot Standby link 7-48
Managing security 7-51
Exiting FIPS 140-2 mode 7-51
Zeroizing critical security parameters 7-51
Displaying login information 7-52
Disabling AES encryption 7-52

Changing AES encryption keys 7-53
Changing the log-out timer 7-56
Managing performance 7-57
Checking system statistics and counters 7-57
Resetting system statistics and counters 7-62
Viewing diagnostics 7-62
Using the diagnostics plotter 7-63
Downloading diagnostic data 7-64
Changing the diagnostics refresh period 7-65
Maintaining the system 7-66
Restoring, upgrading and rebooting 7-67
Restoring the system configuration 7-67
Upgrading software 7-68
Rebooting 7-69
Upgrading software in an operational 1+1 Hot Standby link 7-69
Checking the recovery version 7-70
Using recovery mode 7-71
Entering recovery mode 7-71
Selecting recovery option 7-72
Upgrading software image 7-74
Resetting IP and Ethernet configuration to factory defaults 7-75
Erasing configuration 7-76
Zeroizing security parameters 7-76
Downgrading PTP 800 software 7-77
Chapter 8: Troubleshooting 8-1
Connecting to the web management interface 8-2
Check the CMU power indicator 8-2
Check the DC supply to the CMU 8-2
Check the CMU status indicator 8-3
CMU out of service 8-3
Check the Management port Ethernet connection 8-4
Check the copper Data port Ethernet connection 8-5
Check the fiber Data port Ethernet connection 8-6
Check IP network connection 8-7
Check browser settings 8-8
Installing the link 8-9
Connect to the web management interface 8-9

Check RFU status 8-9
Transmitter status 8-10
Antenna alignment 8-10
Check transmit and receive frequencies 8-11
Check waveguide and antennas 8-11
Check link status 8-11
Check IRFU status LEDs 8-12
Testing protection switchover 8-13
Check protection interface status 8-13
Check that protection switching is enabled 8-13
Check the status of the wireless interface 8-14
Check the link protection cable 8-14
Force a protection switchover 8-14
Check the configuration of the active and inactive units 8-14
Glossary I

List of Figures

Figure 1 Typical PTP 800 deployment (ODU platform) 1-5
Figure 2 Typical PTP 800 deployment (IRFU platform) 1-5
Figure 3 PTP 800 CMU 1-8
Figure 4 CMU front panel 1-9
Figure 5 ODU-A front view 1-14
Figure 6 ODU-B front view 1-15
Figure 7 ODU rear view 1-15
Figure 8 ODU-A side view 1-16
Figure 9 ODU-B side view 1-16
Figure 10 Top and front view of IRFU shelf (with single transceiver and waveguide) 1-18
Figure 11 IRFU 1+0 configuration 1-20
Figure 12 IRFU 1+1 Tx MHSB configuration 1-21
Figure 13 IRFU 1+0 Tx MHSB Ready configuration 1-22
Figure 14 IRFU 1+1 Tx MHSB / Rx SD configuration 1-23
Figure 15 IRFU 2+0 configuration 1-24
Figure 16 IRFU transceiver interfaces 1-25
Figure 17 Typical PTP 800 antenna with ODU (Cambium direct mount interface) 1-27
Figure 18 Direct mount mechanical interface 1-28
Figure 19 ODU clipped onto direct mount mechanical interface 1-28
Figure 20 Remote mount antenna waveguide interface 1-28
Figure 21 RMK showing the ODU interface 1-30
Figure 22 RMK showing the waveguide interface 1-30
Figure 23 ODU coupler mounting kit 1-31
Figure 24 Two ODUs and antenna mounted on a coupler 1-32
Figure 25 Orthogonal mode transducer 1-32
Figure 26 Cable grounding kit for 1/4" and 3/8" cable 1-35
Figure 27 PTP 800 LPU end kit 1-35
Figure 28 Forwarding behavior in out-of-band local management mode 1-47
Figure 29 Forwarding behavior in out-of-band management mode 1-47
Figure 30 Forwarding behavior in in-band mode 1-47
Figure 31 Inactive unit frame forwarding – out-of-band management 1-48

Figure 32 Inactive unit frame forwarding – in-band management 1-48
Figure 33 Protocol layers between Ethernet and wireless interfaces 1-49
Figure 34 Protocol layers between external interfaces and the management agent 1-50
Figure 35 Receive Diversity Ethernet frames 1-67
Figure 36 Tamper evident label on rear edge of CMU 1-70
Figure 37 Indication of FIPS 140-2 capability 1-71
Figure 38 FIPS operational mode alarm 1-71
Figure 39 LINKPlanner profile view 2-5
Figure 40 LINKPlanner configuration and performance details 2-6
Figure 41 LINKPlanner Bill of Materials view 2-6
Figure 42 Rolling sphere method to determine the lightning protection zones 2-8
Figure 43 Grounding and lightning protection on mast or tower 2-12
Figure 44 Grounding and lightning protection on mast or tower (protected end) 2-13
Figure 45 Grounding and lightning protection on building 2-14
Figure 46 Grounding and lightning protection inside high building 2-15
Figure 47 Grounding and lightning protection inside high building (protected end) 2-16
Figure 48 Grounding requirements for the IRFU and CMU 2-17
Figure 49 Schematic view of 1+0 ODU direct mount link end 2-31
Figure 50 Schematic view of 1+0 ODU remote mount link end 2-32
Figure 51 Schematic view of 1+0 IRFU link end 2-33
Figure 52 Schematic view of network connections for a 1+0 link end 2-34
Figure 53 ODUs coupled to single direct mount antenna (schematic) 2-36
Figure 54 ODUs coupled to single remote mount antenna (schematic) 2-37
Figure 55 ODUs with separate direct mount antennas (schematic) 2-38
Figure 56 ODUs with separate remote mount antennas (schematic) 2-39
Figure 57 IRFU 1+1 Tx MHSB with single remote mount antenna (schematic) 2-40
Figure 58 IRFU 1+1 Tx MHSB / Rx SD with two remote mount antennas (schematic) 2-41
Figure 59 Schematic of 1+1 out-of-band network connections (redundant copper or fiber) 2-44
Figure 60 Schematic of 1+1 out-of-band network connections (Fiber-Y) 2-45
Figure 61 Schematic of 1+1 in-band network connections 2-46
Figure 62 ODUs coupled to single direct mount antenna - co-polar links (schematic) 2-50
Figure 63 ODUs coupled to a single remote mount antenna - co-polar links (schematic) 2-51
Figure 64 ODUs coupled to a single direct mount antenna - cross-polar links (schematic) 2-52
Figure 65 ODUs connected to a dual polar remote mount antenna - cross-polar links (schematic) 2-53
Figure 66 IRFU 2+0 with single remote mount antenna (schematic) 2-54
Figure 67 Locations of waveguide flanges 4-10

Figure 68 Waveguide flanges – 6 GHz 4-12
Figure 69 Waveguide flanges – 7 to 15 GHz 4-13
Figure 70 Waveguide flanges – 18 to 38 GHz 4-14
Figure 71 Waveguide flanges – 11 GHz tapered transition 4-14
Figure 72 European Union compliance label 4-85
Figure 73 Dual-polar antenna in remote mount configuration 5-10
Figure 74 Words embossed on coupler (asymmetric shown) 5-21
Figure 75 Correct orientation of LPUs 5-37
Figure 76 ODU and top LPU grounding 5-42
Figure 77 Using the hoist line 5-51
Figure 78 IF cable grounding on a mast or tower 5-52
Figure 79 Grounding at building entry 5-58
Figure 80 Example of a cable analyzer 5-61
Figure 81 Example of the cable test 5-61
Figure 82 Cable loss plot for a 17 meter cable with no ODU 5-63
Figure 83 Cable loss plot for a 17 meter cable with ODU connected 5-64
Figure 84 Cable loss plot for a 100 meter cable with no ODU 5-65
Figure 85 Cable loss plot for a 100 meter cable with ODU connected 5-65
Figure 86 DTF plot for a 17 meter cable with no ODU 5-68
Figure 87 DTF plot for a 17 meter cable with ODU connected 5-69
Figure 88 IRFU rack mounting 5-71
Figure 89 Partial rear view of IRFU with waveguide port 5-72
Figure 90 Connecting the coaxial cable to the IRFU 5-73
Figure 91 IRFU grounding terminal (front option) 5-74
Figure 92 IRFU grounding terminal (rear option) 5-74
Figure 93 IRFU power connection 5-76
Figure 94 CMU kit contents 5-78
Figure 95 CMU mounted on bench 5-79
Figure 96 CMU mounted with bracket 5-79
Figure 97 CMU with rack mounting kit and blanking plate 5-80
Figure 98 CMU mounted in rack 5-80
Figure 99 CMU ground connector 5-81
Figure 100 Rack mounted CMU with a right angled IF cable connector 5-81
Figure 101 Cambium AC to DC converter 5-83
Figure 102 Copper data interface connections 5-85
Figure 103 Fiber data interface connections 5-86
Figure 104 Management interface connections 5-87

Figure 105 Out-of-band protection splitter connections 5-90
Figure 106 Redundant copper interface connections 5-91
Figure 107 Redundant fiber interface connections 5-92
Figure 108 Optical Y interface connections 5-93
Figure 109 Protection cable connections 5-94
Figure 110 IRFU components (example) 5-96
Figure 111 Transceiver replacement (1+0 example) 5-98
Figure 112 Branching unit replacement 5-100
Figure 113 Filter replacement 5-102
Figure 114 Fan assembly replacement 5-103
Figure 115 RF cable installation and removal (1+1 Tx MHSB / Rx SD example) 5-104
Figure 116 LAN Configuration page with VLAN disabled 6-11
Figure 117 Confirm LAN Configuration 6-19
Figure 118 Software License Key page 6-22
Figure 119 Software License Key page with full capacity trial in progress 6-24
Figure 120 Software Version in System Status page 6-26
Figure 121 Installation Configuration page 6-30
Figure 122 Security Configuration Wizard page 6-34
Figure 123 Step 1: Enter Key of Keys page 6-35
Figure 124 Step 2: TLS Private Key and Public Certificate page 6-36
Figure 125 Step 3: User Security Banner page 6-36
Figure 126 Step 4: Login Information Settings page 6-37
Figure 127 Step 5: Random Number Entropy Input page 6-37
Figure 128 Step 6: Enter Wireless Link Encryption Key page 6-38
Figure 129 Step 7: HTTP and Telnet Settings page 6-39
Figure 130 Step 8: Commit Security Configuration page 6-41
Figure 131 Local User Accounts page (identity-based user accounts not shown) 6-43
Figure 132 Identity-based user accounts 6-47
Figure 133 Change Password page 6-49
Figure 134 Webpage Properties page 6-49
Figure 135 RADIUS Configuration page 6-51
Figure 136 Protection Configuration page (protection disabled) 6-53
Figure 137 Protection Configuration page for 1+1 (Primary) 6-56
Figure 138 Protection Configuration page for 1+1 with Rx Diversity (Primary) 6-56
Figure 139 Protection Configuration page for 1+1 (Secondary) 6-57
Figure 140 Protection Configuration page for 1+1 with Rx Diversity (Secondary) 6-57
Figure 141 Current Installation Summary page 6-64

Figure 142 Step 1: Enter equipment details page (ODU) 6-65
Figure 143 Step 1: Enter equipment details page (IRFU) 6-66
Figure 144 Step 2: Radio License Configuration page (fixed modulation) 6-69
Figure 145 Step 2: Radio License Configuration page (FCC adaptive modulation) 6-70
Figure 146 Step 2: Radio License Configuration page (ETSI adaptive modulation) 6-70
Figure 147 Step 3: Wireless Configuration page (normal) 6-72
Figure 148 Step 3: Wireless Configuration page (ETSI adaptive modulation) 6-72
Figure 149 Step 4: Confirm Installation Configuration page 6-74
Figure 150 Step 5: Start Antenna Alignment page 6-75
Figure 151 Step 6: Configuration Complete page (step 5 cancelled) 6-76
Figure 152 Current SNMP Summary page (when SNMP is disabled) 6-77
Figure 153 Step 1: SNMP Configuration page (for SNMPv3) 6-78
Figure 154 Step 2: SNMP MIB-II System Objects page 6-79
Figure 155 Step 3: SNMP User Policy Configuration page (for SNMPv3) 6-80
Figure 156 Step 4: SNMP User Accounts Configuration page (for SNMPv3) 6-82
Figure 157 Step 5: SNMP Trap Configuration page (for SNMPv3) 6-83
Figure 158 Confirm SNMP Configuration page (for SNMPv3) 6-85
Figure 159 Step 1: SNMP Configuration page (for SNMPv1/2c) 6-86
Figure 160 Step 3: SNMP Trap Configuration page (for SNMPv1/2c) 6-87
Figure 161 Confirm SNMP Configuration page (for SNMPv1/2c) 6-89
Figure 162 Diagnostic Alarms page (with protection alarms) 6-91
Figure 163 Email Configuration page 6-92
Figure 164 Syslog Configuration page 6-94
Figure 165 Web-Based Management page 6-96
Figure 166 Step 6: Antenna Alignment page (searching for link) 6-101
Figure 167 Symmetrical relationship between voltage and alignment 6-102
Figure 168 Typical RSSI voltage peaks and troughs 6-103
Figure 169 Step 6: Antenna Alignment page (link established) 6-104
Figure 170 Alignment Abandoned 6-104
Figure 171 Step 7: Installation Complete page 6-105
Figure 172 Installation Configuration page 6-107
Figure 173 QoS Configuration page (Ethernet) 6-111
Figure 174 QoS Configuration page (IP/MPLS) 6-112
Figure 175 Time Configuration page (SNTP disabled) 6-116
Figure 176 Time Configuration page (SNTP enabled) 6-117
Figure 177 Save & Restore Configuration page 6-120
Figure 178 HTTPS key size warning alarm 6-123

Figure 179 System Administration Login page 7-2
Figure 180 Menu and System Summary page (wireless link up) 7-3
Figure 181 System Summary page 7-6
Figure 182 System Status page (unprotected link) 7-8
Figure 183 System Status page (1+1 Hot Standby link) 7-9
Figure 184 Web browser with default title 7-12
Figure 185 Browser Title variable entry 7-13
Figure 186 Identifying units in the web browser title bar and tabs 7-14
Figure 187 Alarm warning triangle 7-15
Figure 188 Syslog local log 7-31
Figure 189 System Configuration page (partial view) when transmitter is muted 7-32
Figure 190 Protected Link page 7-33
Figure 191 Login Information page 7-52
Figure 192 Encryption key mismatch 7-55
Figure 193 Web Page Properties page 7-56
Figure 194 System Statistics and Counters page 7-58
Figure 195 Diagnostics page (1+0 or 2+0 link) 7-62
Figure 196 Diagnostics page (1+1 link) 7-63
Figure 197 Diagnostics Plotter page 7-64
Figure 198 Generate Downloadable Diagnostics page 7-65
Figure 199 Reboot Wireless Unit page 7-69
Figure 200 Recovery Mode Warning page 7-72
Figure 201 Recovery Options page 7-73
Figure 202 Recovery Software Upgrade confirmation page 7-74
Figure 203 Recovery Software Upgrade complete page 7-74
Figure 204 Reset Configuration dialog 7-75
Figure 205 Erase Configuration dialog 7-76
Figure 206 Zeroize Security Parameters dialog 7-77

List of Tables

Table 1 PTP 800 licensed bands and frequencies (ODU-A platform) 1-3
Table 2 PTP 800 licensed bands and frequencies (ODU-B platform) 1-3
Table 3 PTP 800 licensed bands and frequencies (IRFU platform) 1-4
Table 4 CMU interfaces 1-9
Table 5 CMU LED states 1-11
Table 6 ODU interfaces 1-16
Table 7 IRFU transceiver interfaces 1-25
Table 8 HTTPS/TLS security material 2-23
Table 9 Permitted character set for SNMPv3 passphrases 2-26
Table 10 Default SNMPv3 users 2-27
Table 11 Definition of auth-role vendor-specific attribute 2-29
Table 12 Frame size and latency relationship in Rx SD links 2-48
Table 13 Minimum transmit/transmit frequency separation at a 2+0 IRFU link end 2-55
Table 14 Minimum transmit/receive frequency separation at a 2+0 IRFU link end 2-56
Table 15 Optional components for PTP 800 CMUs 2-57
Table 16 Selecting antennas for each hardware configuration 2-59
Table 17 Antennas: 6 GHz single polarization 2-60
Table 18 Antennas: 6 GHz dual polarization 2-60
Table 19 Antennas: 7 GHz and 8 GHz single polarization 2-61
Table 20 Antennas: 7 GHz and 8 GHz dual polarization 2-61
Table 21 Antennas: 11 GHz single polarization 2-62
Table 22 Antennas: 11 GHz dual polarization 2-62
Table 23 Antennas: 13 GHz single polarization 2-63
Table 24 Antennas: 13 GHz dual polarization 2-63
Table 25 Antennas: 15 GHz single polarization 2-64
Table 26 Antennas: 15 GHz dual polarization 2-64
Table 27 Antennas: 18 GHz single polarization 2-65
Table 28 Antennas: 18 GHz dual polarization 2-65
Table 29 Antennas: 23 GHz single polarization 2-66
Table 30 Antennas: 23 GHz dual polarization 2-66
Table 31 Antennas: 26 GHz single polarization 2-67

Table 32 Antennas: 26 GHz dual polarization 2-67
Table 33 Antennas: 28 GHz single polarization 2-67
Table 34 Antennas: 28 GHz dual polarization 2-67
Table 35 Antennas: 32 GHz single polarization 2-68
Table 36 Antennas: 32 GHz dual polarization 2-68
Table 37 Antennas: 38 GHz single polarization 2-68
Table 38 Antennas: 38 GHz dual polarization 2-68
Table 39 Parabolic radomes (optional) 2-69
Table 40 ODUs: Lower 6 GHz ODU-A 2-70
Table 41 ODUs: Upper 6 GHz ODU-A 2-70
Table 42 ODUs: 7 GHz ODU-A 2-71
Table 43 ODUs: 8 GHz ODU-A 2-73
Table 44 ODUs: 11 GHz ODU-B 2-74
Table 45 ODUs: 11 GHz ODU-A 2-75
Table 46 ODUs: 13 GHz ODU-A 2-75
Table 47 ODUs: 15 GHz ODU-A 2-76
Table 48 ODUs: 18 GHz ODU-B 2-77
Table 49 ODUs: 18 GHz ODU-A 2-77
Table 50 ODUs: 23 GHz ODU-B 2-78
Table 51 ODUs: 23 GHz ODU-A 2-78
Table 52 ODUs: 26 GHz ODU-A 2-79
Table 53 ODUs: 28 GHz ODU-A 2-79
Table 54 ODUs: 32 GHz ODU-A 2-79
Table 55 ODUs: 38 GHz ODU-A 2-80
Table 56 Cable and LPU components 2-81
Table 57 Inventory of the coaxial cable installation assembly kit (WB3616) 2-83
Table 58 RMKs, waveguides and accessories 2-85
Table 59 Remote mounting kits 2-86
Table 60 Flexible waveguides 2-87
Table 61 Flex-twist hanger kits available from Cambium 2-88
Table 62 ODU coupler mounting kits 2-88
Table 63 Orthogonal mounting kits (OMKs) 2-90
Table 64 IRFUs – 6 GHz and 11 GHz 2-91
Table 65 IF cable between IRFU and CMU 2-92
Table 66 IRFU transceivers, fan and covers – 6 GHz and 11 GHz 2-93
Table 67 RF cables between transceiver and BU – 6 GHz and 11 GHz 2-93
Table 68 IRFU filter assemblies – 6 GHz and 11 GHz 2-94

Table 69 IRFU upgrade kits – 6 GHz and 11 GHz 2-94
Table 70 Antennas and antenna accessories for IRFU deployments 2-95
Table 71 Copper network cables and connectors 2-96
Table 72 Fiber network cables and connectors 2-96
Table 73 Single-step capacity upgrades (per unit) 2-98
Table 74 Step-by-step capacity upgrades (per unit) 2-98
Table 75 CMU physical specifications 4-2
Table 76 CMU environmental specifications 4-2
Table 77 CMU electrical specifications 4-2
Table 78 ODU and CMU power consumption (ODU-A only) 4-3
Table 79 AC to DC converter specifications 4-4
Table 80 ODU physical specifications 4-5
Table 81 ODU-A and ODU-B environmental specifications 4-5
Table 82 RSSI voltage, received signal level and bandwidth 4-5
Table 83 IRFU physical specifications 4-8
Table 84 IRFU electrical specifications 4-9
Table 85 IRFU environmental specifications 4-9
Table 86 IRFU EMC and safety compliance 4-9
Table 87 IRFU transceiver power consumption 4-10
Table 88 Antenna, transition, waveguide and RMK flanges 4-11
Table 89 Torque value in Nm (lb ft) for each fastener size 4-15
Table 90 ODU coupler physical specifications 4-15
Table 91 ODU coupler environmental specifications 4-15
Table 92 ODU coupler return losses and isolation 4-16
Table 93 ODU coupler insertion losses 4-16
Table 94 Out-of-band protection splitter specifications 4-17
Table 95 Out-of-band protection cable pin outs 4-17
Table 96 Fiber-Y kit specifications 4-18
Table 97 General wireless specifications 4-19
Table 98 ETSI band plan (ODU-A and ODU-B) 4-20
Table 99 FCC and IC band plan (ODU-A and ODU-B) 4-21
Table 100 FCC and IC band plan (IRFU platforms) 4-21
Table 101 NTIA band plan 4-22
Table 102 Brazil band plan 4-22
Table 103 Lower 6 GHz FCC and Canada with 10 MHz bandwidth 4-24
Table 104 Lower 6 GHz FCC and Canada with 30 MHz bandwidth 4-24
Table 105 Lower 6 GHz ETSI with 29.65 MHz channel separation 4-25

Table 106 Upper 6 GHz FCC with 10 MHz bandwidth 4-26
Table 107 Upper 6 GHz FCC with 30 MHz bandwidth 4-26
Table 108 Upper 6 GHz ETSI with 7 MHz channel separation 4-27
Table 109 Upper 6 GHz ETSI with 14 MHz channel separation 4-27
Table 110 Upper 6 GHz ETSI with 30 MHz channel separation 4-27
Table 111 Upper 6 GHz ETSI with 40 MHz channel separation 4-28
Table 112 Upper 6 GHz ETSI with 60 MHz channel separation 4-28
Table 113 6 GHz FCC and Canada with 10 MHz bandwidth for IRFU 4-29
Table 114 6 GHz FCC with 25 MHz bandwidth for IRFU 4-30
Table 115 6 GHz FCC and Canada with 30 MHz bandwidth for IRFU 4-30
Table 116 Transmit branching unit losses for 6 GHz IRFU 4-31
Table 117 Receive branching unit losses for 6 GHz IRFU 4-31
Table 118 7 GHz ETSI with 7 MHz channel separation 4-32
Table 119 7 GHz ETSI with 14 MHz channel separation 4-32
Table 120 7 GHz ETSI with 28 MHz channel separation 4-33
Table 121 8 GHz ETSI with 7 MHz channel separation 4-33
Table 122 8 GHz ETSI with 14 MHz channel separation 4-34
Table 123 8 GHz ETSI with 28 MHz channel separation 4-34
Table 124 8 GHz ETSI with 29.65 MHz channel separation 4-34
Table 125 11 GHz FCC and Canada with 10 MHz bandwidth (ODU-A) 4-35
Table 126 11 GHz FCC and Canada with 10 MHz bandwidth (ODU-B) 4-35
Table 127 11 GHz FCC and Canada with 30 MHz bandwidth (ODU-A) 4-36
Table 128 11 GHz FCC and Canada with 30 MHz bandwidth (ODU-B) 4-36
Table 129 11 GHz FCC and Canada with 40 MHz bandwidth (ODU-A) 4-37
Table 130 11 GHz FCC and Canada with 40 MHz bandwidth (ODU-B) 4-37
Table 131 11 GHz ETSI with 40 MHz channel separation 4-38
Table 132 11 GHz FCC and Canada with 10 MHz bandwidth for IRFU 4-39
Table 133 11 GHz FCC and Canada with 30 MHz bandwidth for IRFU 4-40
Table 134 11 GHz FCC and Canada with 40 MHz bandwidth for IRFU 4-40
Table 135 Transmit branching unit losses for 11 GHz IRFU 4-41
Table 136 Receive branching unit losses for 11 GHz IRFU 4-41
Table 137 13 GHz ETSI with 7 MHz channel separation 4-42
Table 138 13 GHz ETSI with 14 MHz channel separation 4-42
Table 139 13 GHz ETSI with 28 MHz channel separation 4-43
Table 140 15 GHz ETSI with 7 MHz channel separation 4-44
Table 141 15 GHz ETSI with 14 MHz channel separation 4-44
Table 142 15 GHz ETSI with 28 MHz channel separation 4-45

Table 143 15 GHz ETSI with 56 MHz channel separation 4-45
Table 144 18 GHz FCC and Canada with 10 MHz bandwidth (ODU-A) 4-46
Table 145 18 GHz FCC and Canada with 10 MHz bandwidth (ODU-B) 4-46
Table 146 18 GHz FCC and Canada with 20 MHz bandwidth (ODU-A) 4-47
Table 147 18 GHz FCC and Canada with 20 MHz bandwidth (ODU-B) 4-47
Table 148 18 GHz FCC and Canada with 30 MHz bandwidth (ODU-A) 4-48
Table 149 18 GHz FCC and Canada with 30 MHz bandwidth (ODU-B) 4-48
Table 150 18 GHz FCC and Canada with 40 MHz bandwidth (ODU-A) 4-49
Table 151 18 GHz FCC and Canada with 40 MHz bandwidth (ODU-B) 4-49
Table 152 18 GHz FCC and Canada with 50 MHz bandwidth (ODU-A) 4-50
Table 153 18 GHz FCC and Canada with 50 MHz bandwidth (ODU-B) 4-50
Table 154 18 GHz FCC and Canada with 80 MHz bandwidth (ODU-B) 4-51
Table 155 18 GHz ETSI with 7 MHz channel separation 4-51
Table 156 18 GHz ETSI with 13.75 MHz channel separation 4-51
Table 157 18 GHz ETSI with 27.5 MHz channel separation 4-52
Table 158 18 GHz ETSI with 55 MHz channel separation 4-52
Table 159 18 GHz Brazil with 13.75 MHz channel separation 4-53
Table 160 18 GHz Brazil with 27.5 MHz channel separation 4-53
Table 161 18 GHz Brazil with 55 MHz channel separation 4-53
Table 162 23 GHz FCC and Canada with 10 MHz bandwidth (ODU-A) 4-54
Table 163 23 GHz FCC and Canada with 10 MHz bandwidth (ODU-B) 4-55
Table 164 23 GHz FCC and Canada with 20 MHz bandwidth (ODU-A) 4-55
Table 165 23 GHz FCC and Canada with 20 MHz bandwidth (ODU-B) 4-56
Table 166 23 GHz FCC and Canada with 30 MHz bandwidth (ODU-A) 4-56
Table 167 23 GHz FCC and Canada with 30 MHz bandwidth (ODU-B) 4-57
Table 168 23 GHz FCC and Canada with 40 MHz bandwidth (ODU-A) 4-57
Table 169 23 GHz FCC and Canada with 40 MHz bandwidth (ODU-B) 4-58
Table 170 23 GHz FCC and Canada with 50 MHz bandwidth (ODU-A) 4-58
Table 171 23 GHz FCC and Canada with 50 MHz bandwidth (ODU-B) 4-59
Table 172 23 GHz ETSI with 7 MHz channel separation 4-59
Table 173 23 GHz ETSI with 14 MHz channel separation 4-59
Table 174 23 GHz ETSI with 28 MHz channel separation 4-60
Table 175 23 GHz ETSI with 56 MHz channel separation 4-60
Table 176 26 GHz FCC with 10 MHz bandwidth 4-61
Table 177 26 GHz FCC with 20 MHz bandwidth 4-61
Table 178 26 GHz FCC with 40 MHz bandwidth 4-62
Table 179 26 GHz ETSI with 7 MHz channel separation 4-62

Table 180 26 GHz ETSI with 14 MHz channel separation 4-62
Table 181 26 GHz ETSI with 28 MHz channel separation 4-63
Table 182 26 GHz ETSI with 56 MHz channel separation 4-63
Table 183 28 GHz ETSI with 7 MHz channel separation 4-64
Table 184 28 GHz ETSI with 14 MHz channel separation 4-64
Table 185 28 GHz ETSI with 28 MHz channel separation 4-65
Table 186 28 GHz ETSI with 56 MHz channel separation 4-65
Table 187 32 GHz ETSI with 7 MHz channel separation 4-66
Table 188 32 GHz ETSI with 14 MHz channel separation 4-66
Table 189 32 GHz ETSI with 28 MHz channel separation 4-67
Table 190 32 GHz ETSI with 56 MHz channel separation 4-67
Table 191 38 GHz FCC and Canada with 10 MHz bandwidth 4-68
Table 192 38 GHz FCC and Canada with 50 MHz bandwidth 4-68
Table 193 38 GHz ETSI with 7 MHz channel separation 4-69
Table 194 38 GHz ETSI with 14 MHz channel separation 4-69
Table 195 38 GHz ETSI with 28 MHz channel separation 4-70
Table 196 38 GHz ETSI with 56 MHz channel separation 4-70
Table 197 Copper data port specifications 4-71
Table 198 Fiber data port specifications 4-71
Table 199 Management port specifications 4-71
Table 200 Ethernet bridging specifications 4-72
Table 201 Event messages 4-74
Table 202 Standard SNMP objects 4-77
Table 203 Identification of interfaces 4-79
Table 204 Counters for the wireless interface 4-79
Table 205 Counters for the data interface 4-80
Table 206 Counters for the management interface 4-80
Table 207 Supported standard notifications 4-81
Table 208 Electrical safety specifications 4-82
Table 209 EMC immunity compliance specifications 4-82
Table 210 PTP 800 minimum separation distances, ETSI method 4-87
Table 211 PTP 800 minimum separation distances, FCC method (ODU) 4-89
Table 212 PTP 800 minimum separation distances, FCC method (IRFU) 4-89
Table 213 Tools required for PTP 800 installation 5-3
Table 214 Selecting antenna and ODU installation procedures 5-5
Table 215 Expected cable loss when ODU is not connected 5-66
Table 216 Tools required for IRFU installation 5-70

Table 217 IRFU waveguide and flange specifications 5-73
Table 218 Selecting network interfaces for 1+1 Hot Standby links 5-89
Table 219 Tools required for IRFU component replacement 5-97
Table 220 RF cable connections (1+1 Tx MHSB / Rx SD example) 5-105
Table 221 IP interface attributes 6-12
Table 222 Management port attributes 6-14
Table 223 Data port attributes 6-16
Table 224 Bridged Ethernet traffic attributes 6-18
Table 225 Capability summary attributes 6-22
Table 226 HTTP and Telnet attributes 6-40
Table 227 Local User account management attributes 6-44
Table 228 Password complexity configuration attributes 6-45
Table 229 Identity-based user accounts attributes 6-48
Table 230 RADIUS Authentication attributes 6-52
Table 231 Protection Configuration attributes 6-58
Table 232 Step 1: Equipment Configuration attributes 6-66
Table 233 Step 2: Radio License Configuration attributes 6-71
Table 234 Step 3: Wireless Configuration attributes 6-72
Table 235 Step 1: SNMP Configuration attributes (for SNMPv3) 6-78
Table 236 Step 2: SNMP MIB-II System Objects attributes 6-79
Table 237 Step 3: SNMP User Policy Configuration attributes (for SNMPv3) 6-81
Table 238 Step 3: SNMP User Accounts Configuration attributes (for SNMPv3) 6-82
Table 239 Step 5: SNMP Trap Configuration attributes (for SNMPv3) 6-83
Table 240 Step 1: SNMP Configuration attributes (for SNMPv1/2c) 6-86
Table 241 Step 3: SNMP Trap Configuration attributes (for SNMPv1/2c) 6-88
Table 242 Email Configuration attributes 6-93
Table 243 Syslog Configuration attributes 6-95
Table 244 Web-Based Management attributes 6-97
Table 245 System Configuration attributes 6-108
Table 246 Layer 2 Control Protocols 6-113
Table 247 Ethernet Priority Queue settings 6-113
Table 248 Manual clock attributes 6-116
Table 249 SNTP clock attributes 6-118
Table 250 Procedures performed from each menu option 7-4
Table 251 System Summary attributes 7-6
Table 252 RFU Status attribute values 7-10
Table 253 Transmitter Status attribute values 7-10

Table 254 Wireless Link Status attribute values 7-11
Table 255 Transmit Modulation Selection Detail attribute values 7-11
Table 256 Data Port Status attribute values 7-12
Table 257 Management Port Status attribute values 7-12
Table 258 Browser Title attribute variables 7-13
Table 259 SNMP traps supported by PTP 800 7-24
Table 260 Protected Link page symbols and text 7-34
Table 261 System Statistics and Counters attributes 7-59
Table 262 Recovery options 7-73
Table 263 CMU power indicator checks 8-2
Table 264 DC supply checks when CMU power indicator is off 8-2
Table 265 CMU status indicator checks 8-3
Table 266 Management port indicator checks 8-4
Table 267 Copper Data port indicator checks 8-5
Table 268 Fiber Data port indicator checks 8-6
Table 269 Ping response checks 8-8
Table 270 RFU status checks 8-9
Table 271 Transmitter Status checks 8-10
Table 272 Link Status checks 8-11
Table 273 IRFU LED status checks 8-12
Table 274 Protected Interface Status values and actions 8-13

About This User Guide

This guide describes the planning, installation and operation of the Cambium PTP 800. It is intended for use by the system designer, system installer and the system administrator.

Users of this guide should have knowledge of the following areas:

- Radio network design
- Outdoor radio equipment installation
- System installation, configuration, monitoring and fault finding

System designers should refer to the following chapters:

- Chapter 1: Product description
- Chapter 2: Planning considerations
- Chapter 3: Legal information
- Chapter 4: Reference information

Installers should refer to the following chapters:

- Chapter 5: Installation
- Chapter 6: Configuration and alignment
- Chapter 8: Troubleshooting

Operators should refer to the following chapters:

- Chapter 1: Product description
- Chapter 6: Configuration and alignment
- Chapter 7: Operation
- Chapter 8: Troubleshooting

General information

Version information

The following shows the issue status of this document:

Document issue	Date of issue	Remarks
001v000	Apr 2012	System Release 800-05-00
002v000	May 2012	System Release 800-05-00 (minor revision)
003v000	Jul 2012	System Release 800-05-01
004v000	Oct 2012	System Release 800-05-02

Contacting Cambium Networks

Support website:	http://www.cambiumnetworks.com/support
Main website:	http://www.cambiumnetworks.com
Sales enquiries:	solutions@cambiumnetworks.com
Support enquiries:	support@cambiumnetworks.com
Telephone number list:	http://www.cambiumnetworks.com/contact.php
Address:	Cambium Networks Limited, Linhay Business Park, Eastern Road, Ashburton, Devon, UK, TQ13 7UP

Purpose

Cambium Networks Point-To-Point (PTP) documents are intended to instruct and assist personnel in the operation, installation and maintenance of the Cambium PTP equipment and ancillary devices. It is recommended that all personnel engaged in such activities be properly trained.

Cambium disclaims all liability whatsoever, implied or express, for any risk of damage, loss or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf, to abide by the instructions, system parameters, or recommendations made in this document.

Cross references

References to external publications are shown in italics. Other cross references, emphasized in blue text in electronic versions, are active links to the references.

This document is divided into numbered chapters that are divided into sections. Sections are not numbered, but are individually named at the top of each page, and are listed in the table of contents.

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. Send feedback to support@cambiumnetworks.com.

Problems and warranty

Reporting problems

If any problems are encountered when installing or operating this equipment, follow this procedure to investigate and report:

1. Search this document and the software release notes of supported releases.
2. Visit the support website.
3. Ask for assistance from the Cambium product supplier.
4. Gather information from affected units, such as any available diagnostic downloads.
5. Escalate the problem by emailing or telephoning support.

Repair and service

If unit failure is suspected, obtain details of the Return Material Authorization (RMA) process from the support website.

Warranty

Cambium's standard hardware warranty is for one (1) year from date of shipment from Cambium or a Cambium distributor. Cambium warrants that hardware will conform to the relevant published specifications and will be free from material defects in material and workmanship under normal use and service. Cambium shall within this time, at its own option, either repair or replace the defective product within thirty (30) days of receipt of the defective product. Repaired or replaced product will be subject to the original warranty period but not less than thirty (30) days.

To register PTP products or activate warranties, visit the support website.

For warranty assistance, contact the reseller or distributor.

⚠ CAUTION

Using non-Cambium parts for repair could damage the equipment or void warranty. Contact Cambium for service and repair instructions.

⚠ CAUTION

Portions of Cambium equipment may be damaged from exposure to electrostatic discharge. Use precautions to prevent damage.

Security advice

Cambium Networks systems and equipment provide security parameters that can be configured by the operator based on their particular operating environment. Cambium recommends setting and using these parameters following industry recognized security practices. Security aspects to be considered are protecting the confidentiality, integrity, and availability of information and assets. Assets include the ability to communicate, information about the nature of the communications, and information about the parties involved.

In certain instances Cambium makes specific recommendations regarding security practices, however the implementation of these recommendations and final responsibility for the security of the system lies with the operator of the system.

Warnings, cautions, and notes

The following describes how warnings and cautions are used in this document and in all documents of the Cambium Networks document set.

Warnings

Warnings precede instructions that contain potentially hazardous situations. Warnings are used to alert the reader to possible hazards that could cause loss of life or physical injury. A warning has the following format:

WARNING

Warning text and consequence for not following the instructions in the warning.

Cautions

Cautions precede instructions and are used when there is a possibility of damage to systems, software, or individual items of equipment within a system. However, this damage presents no danger to personnel. A caution has the following format:

CAUTION

Caution text and consequence for not following the instructions in the caution.

Notes

A note means that there is a possibility of an undesirable situation or provides additional information to help the reader understand a topic or concept. A note has the following format:

NOTE

Note text.

Caring for the environment

The following information describes national or regional requirements for the disposal of Cambium Networks supplied equipment and for the approved disposal of surplus packaging.

In EU countries

The following information is provided to enable regulatory compliance with the European Union (EU) directives identified and any amendments made to these directives when using Cambium equipment in EU countries.



Disposal of Cambium equipment

European Union (EU) Directive 2002/96/EC Waste Electrical and Electronic Equipment (WEEE)

Do not dispose of Cambium equipment in landfill sites. In the EU, Cambium in conjunction with a recycling partner ensures that equipment is collected and recycled according to the requirements of EU environmental law.

Disposal of surplus packaging

Do not dispose of surplus packaging in landfill sites. In the EU, it is the individual recipient's responsibility to ensure that packaging materials are collected and recycled according to the requirements of EU environmental law.

In non-EU countries

In non-EU countries, dispose of Cambium equipment and all surplus packaging in accordance with national and regional regulations.

Licensing requirements

Operating license

This equipment operates in bands that require a license in most countries.

⚠ CAUTION

In most countries it is illegal to operate the PTP 800 without a license from the regional or local regulating authority.

United States of America

This device has been verified by Cambium Networks as being in compliance with the requirements of the rules of the Federal Communications Commission (FCC), 47 C.F.R. Part 101, and may not be operated without a station license. In the United States such licenses are issued by the FCC to entities other than agencies of the United States government. Federal government agencies are licensed by the National Telecommunications and Information Administration (NTIA) acting upon the recommendation of the Interdepartment Radio Advisory Committee (IRAC).

Cambium license agreement

The PTP 800 must be operated in accordance with the Cambium Networks end user license agreement, as specified in Chapter 3: Legal information.

Chapter 1: Product description

This chapter provides a high level description of the PTP 800 product. It describes in general terms the function of the product, the main product variants and typical deployment. It also describes the main hardware components.

The following topics are described in this chapter:

- Overview on page 1-2 introduces the key features, typical uses, product variants and components of the PTP 800.
- Compact modem unit (CMU) on page 1-8 describes the CMU and its interfaces.
- Outdoor unit (ODU) on page 1-13 describes the ODU and its interfaces.
- Indoor RF unit (IRFU) on page 1-18 describes the IRFU and its interfaces.
- Antennas and couplers on page 1-27 describes the PTP 800 antennas, couplers and remote mounting kit.
- Cabling and lightning protection on page 1-34 describes the cabling and lightning protection components of a PTP 800 installation.
- Wireless operation on page 1-37 describes how the PTP 800 wireless link is operated, including modulation modes, power control and security.
- Ethernet bridging on page 1-42 describes how the PTP 800 controls Ethernet data, in both the customer data network and the system management network.
- System management on page 1-51 introduces the PTP 800 management system, including the web interface, installation, configuration, alerts and upgrades.
- 1+1 Hot Standby link protection on page 1-64 describes the concept, operation and interfaces of 1+1 Hot Standby links.
- FIPS 140-2 on page 1-70 describes the (optional) FIPS 140-2 cryptographic mode of operation.

Overview

Cambium PTP 800 Licensed Ethernet Microwave products are designed for Ethernet bridging at up to 368 Mbps over licensed point-to-point microwave links in selected licensed bands from 6 GHz to 38 GHz. The products offer exceptional cost efficiency and scalability.

Key features

The key features of the PTP 800 include:

- Support for licensed bands from 6 GHz to 38 GHz.
- Link capacity from 10 Mbps to 368 Mbps in each direction.
- Configurable channel bandwidths from 7 MHz to 80 MHz (FCC and ETSI).
- Upgradeable link capacity limits from 10 Mbps to full capacity via software license key, purchased for each end to allow asymmetric link capacity.
- Fixed modulation modes QPSK to 256 QAM.
- Hitless adaptive modulation, the instantaneous capacity adapting to the varying radio conditions.
- Optional 1+1 Hot Standby link protection.
- Optional Receive Spatial Diversity.
- Effective quality of service (QoS), with Layer 2 or Layer 3 classification and eight queues.
- Ultra-low latency, <115 us @ 368 Mbps with 64 byte frames.
- Split mount architecture with a compact indoor unit and a separate RF unit, either outdoor or indoor.
- All indoor solution with 19" rack mounted Indoor Radio Frequency Unit(IRFU).
- In-band or out-of-band network management.
- Link planning with the PTP LINKPlanner.
- Optional FIPS-197 128/256bit AES encryption.
- Optional HTTPS/TLS security on the web-based management interface.
- SNMPv3 with optional AES privacy and SHA1 authentication.
- Full capacity trial for the first 60 days.

Supported bands and frequencies

The PTP 800 outdoor unit (ODU) platform supports the licensed bands and frequencies listed in Table 1 (ODU-A) or Table 2 (ODU-B). The PTP 800 indoor RF unit (IRFU) platform supports the licensed bands and frequencies listed in Table 3.

Table 1 PTP 800 licensed bands and frequencies (ODU-A platform)

Licensed band	Regions	Frequency coverage
Lower 6 GHz	FCC, IC, ETSI	5.925 – 6.425 GHz
Upper 6 GHz	FCC, ETSI	6.425 – 7.125 GHz
7 GHz	ETSI, NTIA	7.110 – 7.9 GHz
8 GHz	ETSI, NTIA	7.725 – 8.5 GHz
11 GHz	FCC, IC, ETSI	10.7 – 11.7 GHz
13 GHz	ETSI	12.75 – 13.25 GHz
15 GHz	ETSI, Mexico, ANZ	14.4 GHz – 15.35 GHz
18 GHz	FCC, IC, ETSI, Brazil	17.7 – 19.7 GHz
23 GHz	FCC, IC, ETSI	21.2 – 23.6 GHz
26 GHz	FCC, ETSI	24.25 – 26.5 GHz
28 GHz	ETSI	27.5 – 29.5 GHz
32 GHz	ETSI	31.8 – 33.4 GHz
38 GHz	FCC, IC, ETSI	37 – 40 GHz

Table 2 PTP 800 licensed bands and frequencies (ODU-B platform)

Licensed band	Regions	Frequency coverage
11 GHz	FCC	10.7 – 11.7 GHz
18 GHz	FCC	17.7 – 19.7 GHz
23 GHz	FCC	21.2 – 23.6 GHz

Table 3 PTP 800 licensed bands and frequencies (IRFU platform)

Licensed band	Regions	Frequency coverage
Lower 6 GHz	FCC, IC	5.925 – 6.425 GHz
Upper 6 GHz	FCC	6.525 – 6.875 GHz
7 GHz	FCC	6.875 – 7.125 GHz
11 GHz	FCC	10.70 – 11.71 GHz
11 GHz	IC	10.696 – 11.71 GHz

Typical users and applications

PTP 800 links may be used to provide high-performance Ethernet communication for:

- Enterprises
- Internet Service Providers (ISPs)
- Government agencies
- Cellular carriers
- Health care and hospitals
- Schools and universities
- Municipalities
- Public safety agencies

PTP 800 systems serve a wide variety of enterprise and network applications, including:

- Building-to-building connectivity
- Leased-line replacement
- Video surveillance
- Network redundancy
- WiMAX, LTE and 3G backhaul
- Data overlay networks
- Last mile access and connection

System components

The main components of the PTP 800 are shown in Figure 1 (ODU platform) and Figure 2 (IRFU platform).

Figure 1 Typical PTP 800 deployment (ODU platform)

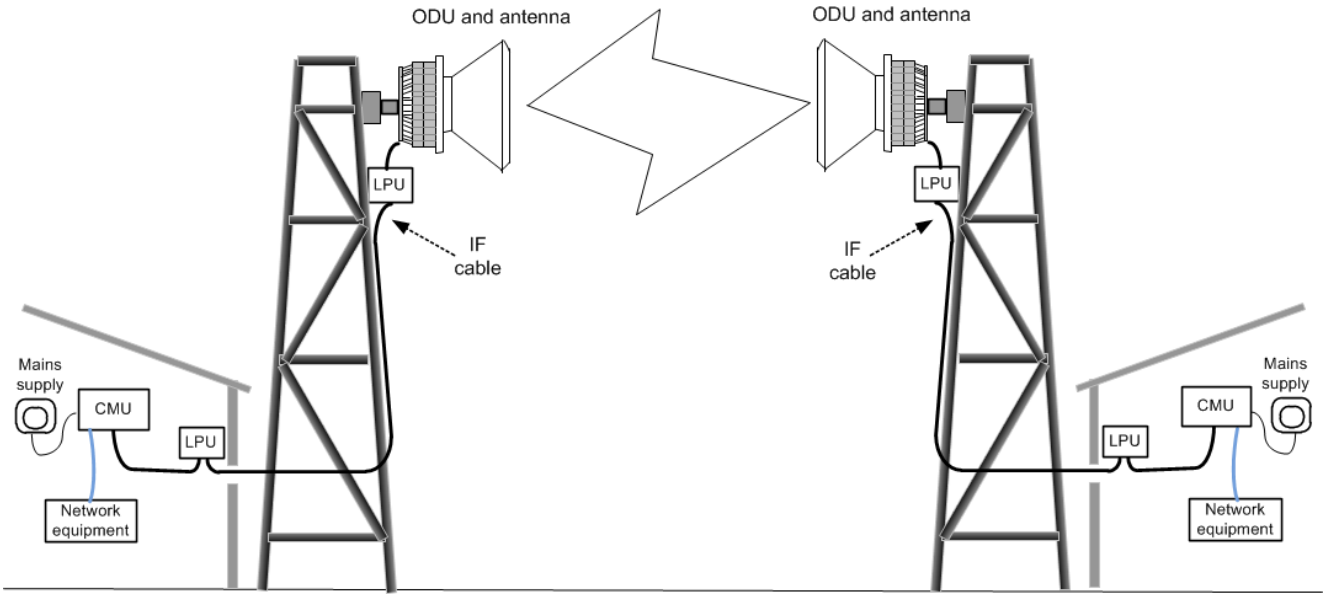
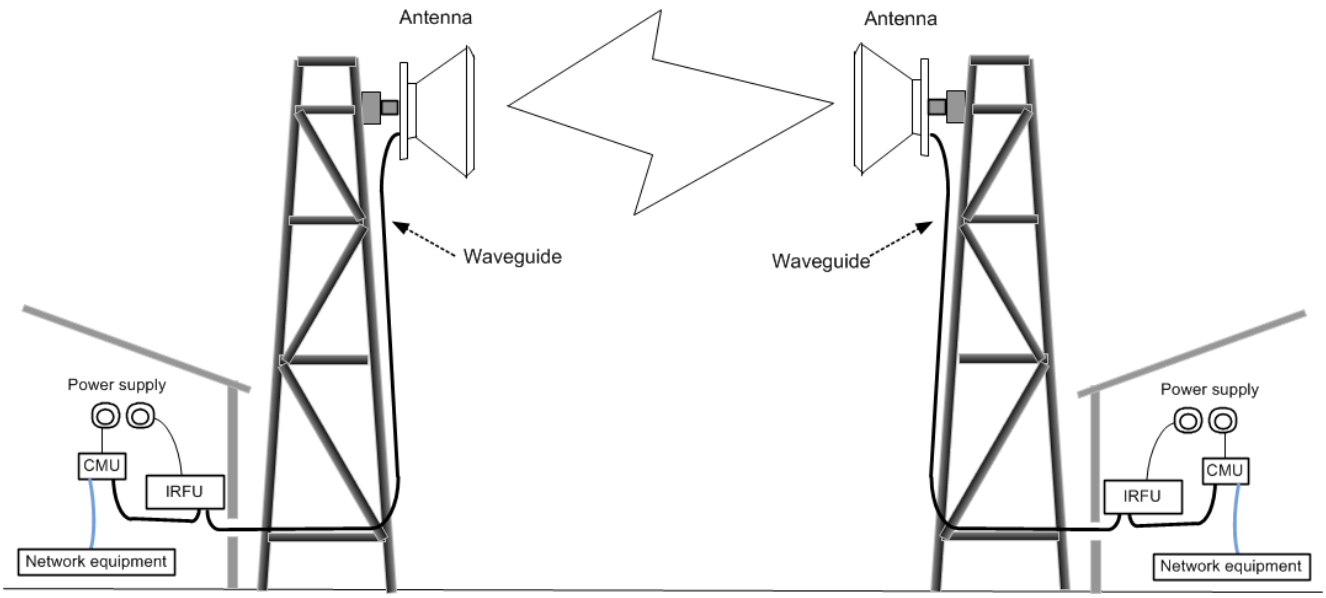


Figure 2 Typical PTP 800 deployment (IRFU platform)



The main components are:

- **Compact modem unit (CMU)**: The CMU converts data signals between Ethernet frames and a modulated intermediate frequency (IF) carrier.
- **Outdoor unit (ODU)**: The ODU converts signals between a modulated intermediate frequency (IF) and radio band frequencies.
- **Indoor RF unit (IRFU)**: The IRFU is an alternative to the ODU. It is installed indoors, for easier maintenance and security.
- **Antennas and couplers**: Cambium supplies high performance, low profile antennas for PTP 800 frequency bands in sizes from 0.3 m (1 ft) to 3.7 m (12 ft). These can be mounted directly to the ODUs, or remotely via waveguide. In 1+1 links, ODUs installed at the same end can share an antenna through the use of coupler mounting kits.
- **Cabling and lightning protection**:
  - ODU platforms: The CMU is connected to the ODU using CNT-400 coaxial cable (IF cable), lightning protection units (LPUs) and grounding cables.
  - IRFU platforms: The IRFU is connected to the antenna using flexible waveguide and premium elliptical waveguide.



The generic term RFU is used in this user guide (and in the web interface) to include the ODU and IRFU.

Link types

The PTP 800 supports the following link types:

- **1+0 single link**: A 1+0 single link transports Ethernet frames between two sites. Each link end has one CMU, one RFU and one antenna.
- **1+1 Hot Standby lin**k: A 1+1 Hot Standby link transports Ethernet frames between two sites and provides protection against single point equipment failure. This is achieved by the deployment of extra equipment which can automatically take over the operation of the link in case of equipment failure. Each end of the link requires two CMUs, either one or two antennas and either two ODUs for outdoor deployments or a 1+1 capable IRFU for indoor deployments. A 1+1 Hot Standby Link can also be configured to support Receive Spatial Diversity which requires two antennas at each end of the link. For indoor deployments, a 1+1 Rx SD capable IRFU is required.
- **2+0 two links sharing antennas**: A 2+0 configuration consists of two 1+0 links between the same two sites, where the antenna at each site is shared between the two 1+0 links. In this user guide and in PTP LINKPlanner, these two links are called link ‘A’ and link ‘B’. Link A and link B must operate on different frequencies and will generally require separate radio licenses. The antennas in a 2+0 link may be single-polar or dual-polar.

For more information about these link types refer to:

- Planning 1+0 links on page 2-30
- Planning 1+1 Hot Standby links on page 2-35
- Planning 2+0 links on page 2-49

Compact modem unit (CMU)

This section describes the PTP 800 CMU and its interfaces.

CMU description

The PTP 800 compact modem unit (CMU) (Figure 3) is mounted indoors and provides the Ethernet interface to the network. It converts the Ethernet frames to a data stream which then modulates an intermediate frequency (IF) signal which is sent to the radio frequency unit (RFU), either an outdoor unit (ODU) or an indoor radio frequency unit (IRFU).

In the other direction, the CMU demodulates a similar IF signal from the RFU and reconstructs Ethernet frames to send to the network. Both IF signals are carried over a coaxial IF cable connecting the CMU to the RFU. The CMU also provides power to the ODU and this is also carried over the coaxial cable. The IRFU is powered separately.

The CMU is mounted on a shelf, on a wall (using the provided bracket), or in a standard 19 inch rack (using the optional CMU rack mounting kit). It is ideally suited to applications where space is limited.

Figure 3 PTP 800 CMU



CMU interfaces

The CMU front panel interfaces are illustrated in Figure 4 and described in Table 4. The CMU front panel indicator LEDs and their states are described in Table 5.

Figure 4 CMU front panel



Table 4 CMU interfaces

Interface	Function
ODU	This is a standard N-type female connector, used to connect the CMU to the ODU or IRFU transceiver via IF cable. The IF cable carries the following multiplexed signals: Power supply at –48 V dc Transmit signal at 350 MHz Receive signal at 140 MHz RFU control and status signals **⚠ CAUTION** Do not connect or disconnect the IF cable when the –48 V supply is applied to the CMU.
Management	This is a 10baseT and 100baseT Ethernet port, used to connect the CMU to the management network when 'out-of-band' management is implemented. It is not used when 'in-band' management is implemented. For more information on the Ethernet interfaces see Data network specifications on page 4-71. For 1+1 Hot Standby protection, spare pins in the management port provide the protection interface between the two CMUs at one end of a link. For more information see 1+1 Hot Standby link protection on page 1-64.

Interface	Function
Recovery	This switch is used to start the CMU in recovery mode. Recovery mode provides a means to recover from serious configuration errors including lost or forgotten passwords and unknown IP addresses. For more information see Recovery mode on page 1-62. Recovery mode also allows new main application software to be loaded even when the integrity of the existing main application software has been compromised.
Data (copper port)	This is a 100baseT and 1000baseT Ethernet port, used to connect the CMU to the customer data network. In the 'in-band' management mode, the system is managed through the Data port and management traffic is multiplexed with customer traffic. For more information on Ethernet interfaces see Data network specifications on page 4-71.
Data (fiber SFP port)	This is a standard small form-factor pluggable (SFP) gigabit interface, used to connect the CMU to the customer data network via a fiber-optic module. When a supported SFP module is present and is working, and the fiber carrier is present, the customer traffic network (and in-band management network, if enabled) connects through fiber, and the copper data port is not used. If the fiber link fails or loses the carrier signal, the Ethernet service falls back to the copper LAN connection. The fiber SFP port is a Class 1 laser product, safe under all conditions of normal operation. For more information on Ethernet interfaces see Wireless specifications on page 4-19.
-48V DC Power	This a socket for connecting the CMU to a standard –48 V dc telecommunications supply, with supply range –40.5 V to –60 V. The 0 V (positive connection) is grounded at the CMU casing, IF cable outer shield and ODU casing.
Ground stud	This M5 ground stud is used to ground the CMU via the supplied lug. The ground cable is fitted to a low impedance ground point. This protects personnel and equipment from hazardous voltages caused by lightning strikes. For a 1+1 Hot Standby protected link, both CMUs are connected to a common ground.

Table 5 CMU LED states

Indicator	State	Description
ODU	Green steady	RFU ready for use and transmitting
	Green slow blink	RFU available for use but muted, or RFU incompatible with radio license configuration
	Red steady	No response from, or incompatible RFU
	Off	RFU not powered
1+1 Management	Green steady	CMU active and protected
	Green blink	CMU on standby and protecting the link
	Orange steady	CMU active but not protected
	Orange blink	CMU is not protecting the link
	Off	The link is not 1+1 Hot Standby
10/100 Management	Orange steady	Ethernet link up, no traffic
	Orange blink	Ethernet link up, traffic
	Off	Ethernet link down or not connected
100 Data	Orange steady	100baseT Ethernet link up, no traffic
	Orange blink	100baseT Ethernet link up, traffic
	Off	Ethernet link down or not 100baseT
1000 Data	Green steady	1000baseT Ethernet link up, no traffic
	Green blink	1000baseT Ethernet link up, traffic
	Off	Ethernet link down or not 1000baseT
GigE Data	Green steady	Fiber Ethernet link up, no traffic
	Green blink	Fiber Ethernet link up, traffic
	Off	Ethernet link down or not connected
Modem	Green steady	Normal operation
	Green slow blink	Wireless link down
	Orange steady	CMU booting
	Red steady	Out of service
	Red slow blink	Recovery mode
	Off	Power supply fault (there may still be power to the CMU)
Power	Green steady	Power supply correct
	Off	Power supply fault (there may still be power to the CMU)

Further reading on the CMU

For more information on the CMU, refer to the following:

- Power supply considerations on page 2-4 describes how to plan the power supply to the PTP 800 CMU.
- Ordering CMUs on page 2-57 describes how to order CMUs for the link and specifies the Cambium part number of the CMU kit.
- CMU specifications on page 4-2 contains specifications of the CMU, such as dimensions, weight and environmental requirements.
- Installing the CMU on page 5-77 describes how to install and connect the CMU.
- Preparing network connections (1+0 and 2+0 links) on page 5-84 describes how to prepare the CMU network connections for unprotected links.
- Preparing network connections (1+1 Hot Standby) on page 5-89 describes how to prepare the CMU network connections for protected links.
- Connecting to the network on page 6-114 describes how to complete and test the CMU network connections.

Outdoor unit (ODU)

This section describes the PTP 800 ODU and its interfaces.

ODU description

The PTP 800 outdoor unit (ODU) provides the necessary frequency conversion and amplification of signals which pass between the CMU and antenna.

In the transmit direction, the ODU takes the fixed intermediate frequency (IF) signal provided by the CMU and converts and amplifies it to a configured licensed band radio frequency signal for transmission at the antenna. In the receive direction, the ODU provides amplification and down conversion of a licensed band signal received at the antenna interface. The result is a fixed IF signal which is passed to the CMU for demodulation.

ODUs are available in all licensed bands supported by PTP 800 (see Supported bands and frequencies on page 1-3 for the full list of supported bands). A given licensed band is generally split into sub-bands where a given sub-band is supported by a pair of ODUs. One ODU is designed to transmit at the high frequency side of the Frequency Division Duplex (FDD), the other at the low frequency side. The ODU transmit and receive frequencies are configurable within a sub-band.

The ODU is designed for outdoor operation, either mounting directly to the back of an antenna or mounted separately using a Remote Mount Kit which then connects to the antenna with flexible waveguide.

The ODU also provides an interface which allows the installer to monitor the receive signal level when aligning antennas.

Alternative ODU platforms

There are two alternative ODU platforms: ODU-A and ODU-B. The platform can be identified from the label.

ODU-A is available in all bands, whereas ODU-B is only available in selected regions and bands. ODU-B is the preferred choice when available, as it offers the following advantages over ODU-A: higher transmit power and lower power dissipation.

⚠ CAUTION

Do not install an ODU-A and an ODU-B in the same link.

For more information about the capabilities and availability of ODU-A and ODU-B, refer to Ordering ODUs on page 2-69.

> **NOTE**
> The term ‘ODU’ covers both ODU-A and ODU-B.

ODU interfaces

The ODU interfaces are illustrated in: Figure 5, Figure 6, Figure 7, Figure 8 and Figure 9. They are described in Table 6.

Figure 5 ODU-A front view

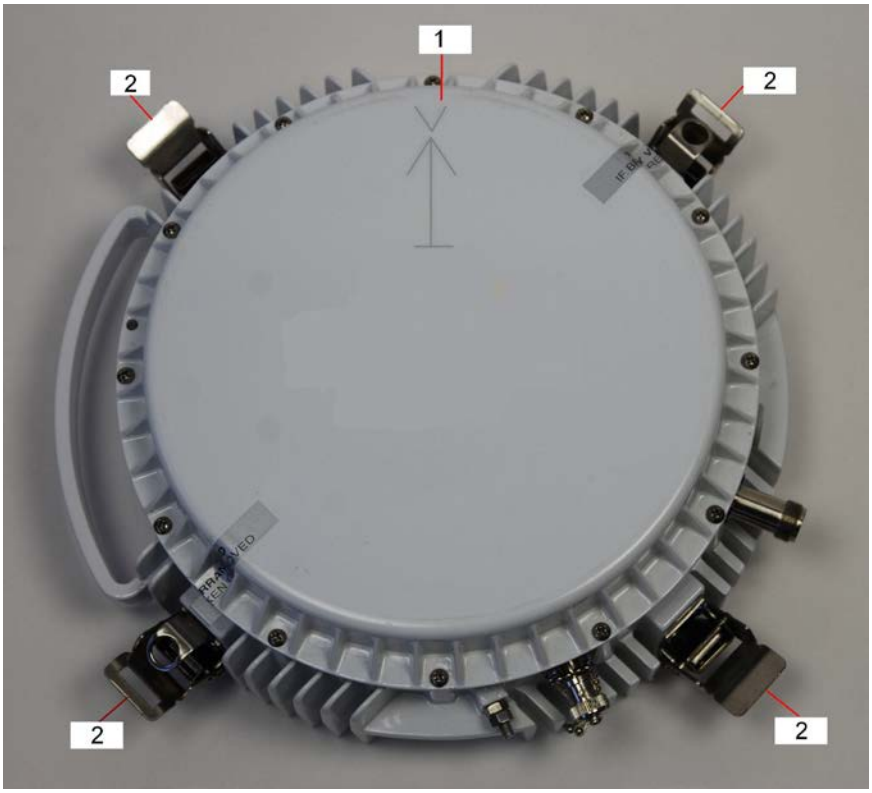


Figure 6 ODU-B front view

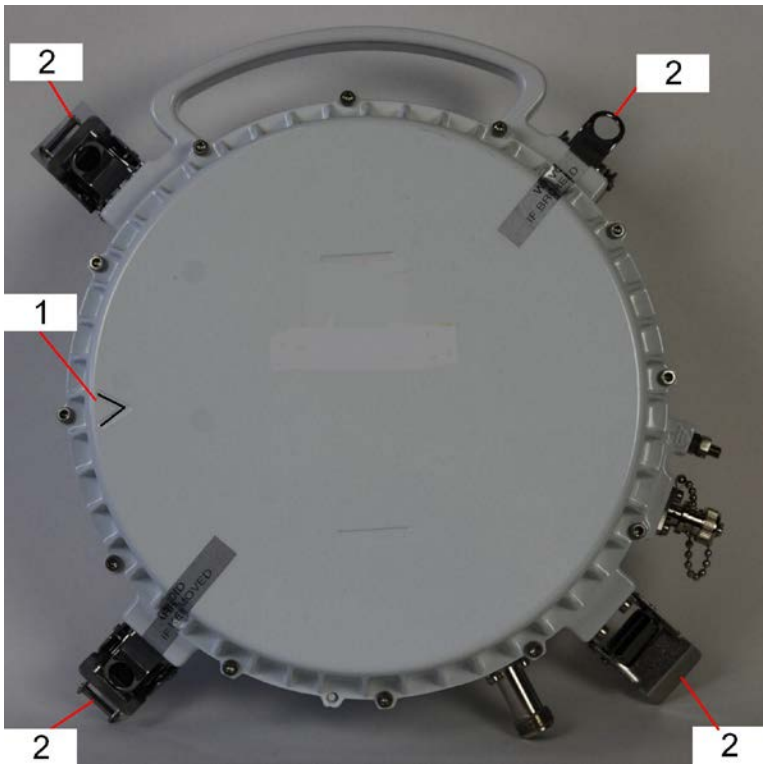


Figure 7 ODU rear view

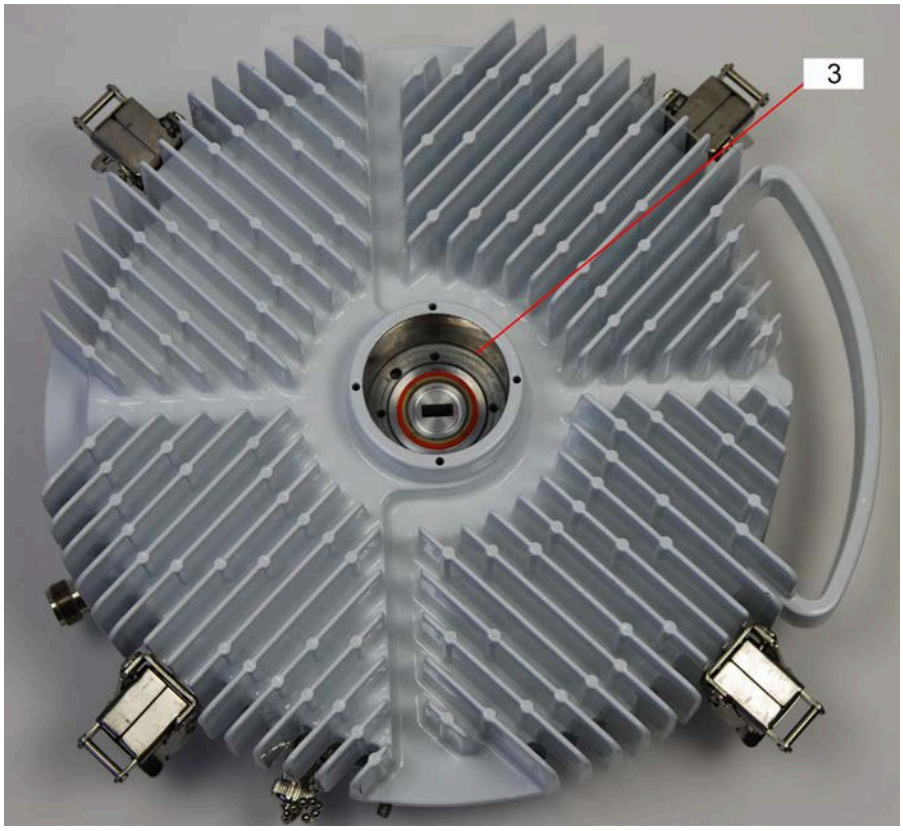


Figure 8 ODU-A side view

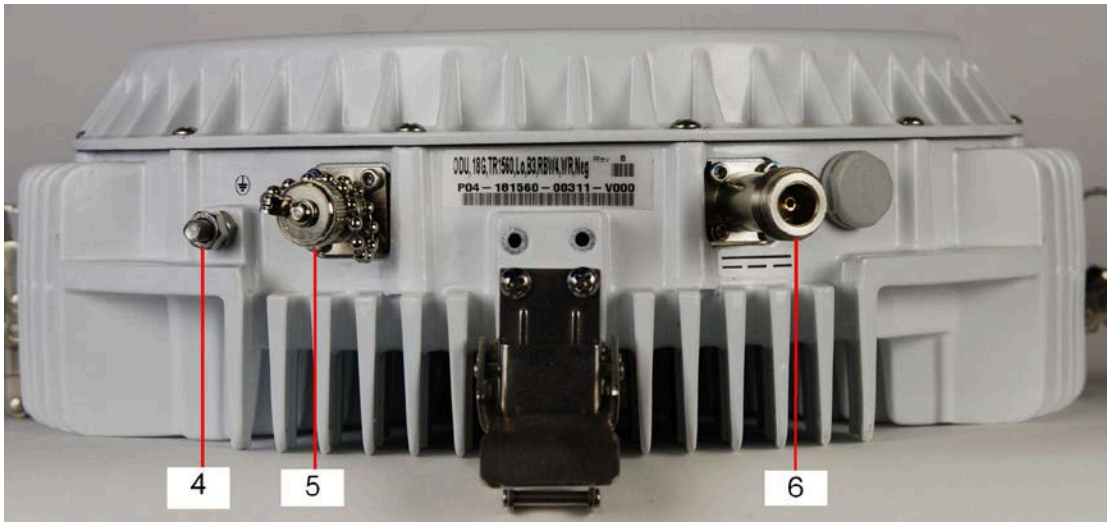


Figure 9 ODU-B side view

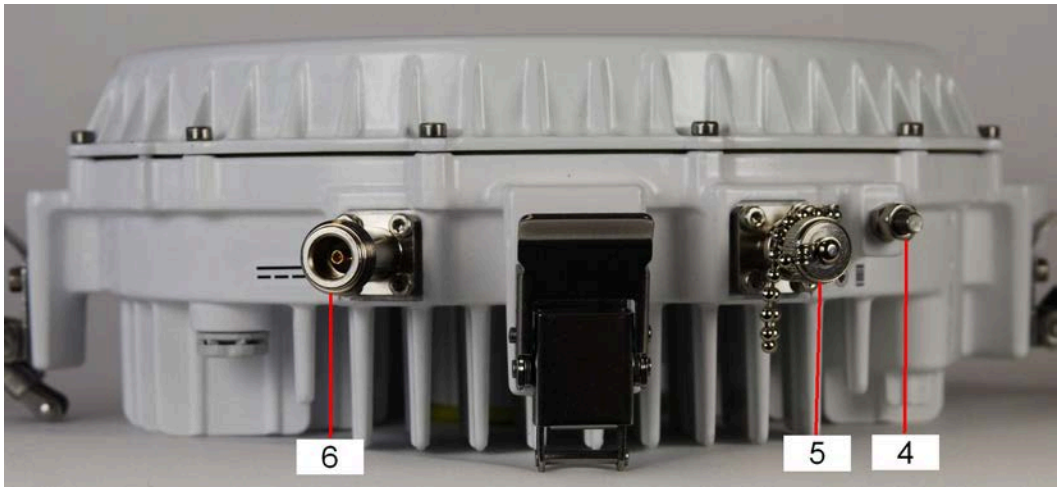


Table 6 ODU interfaces

#	Interface	Function
1	Waveguide polarization arrow	This indicates the orientation of the waveguide interface. The arrow is parallel to the short dimension of the rectangular waveguide aperture.
2	Spring loaded latches	These four spring loaded latches are used to fasten the ODU to the antenna, remote mounting kit or coupler.
3	Waveguide interface	This connects to a Cambium direct mount antenna, an ODU coupler kit, or a remote mounting kit.

#	Interface	Function
4	Ground connector	This is used to ground the ODU to the top lightning protection unit (LPU).
5	RSSI connector	The received signal strength indication (RSSI) connector is a standard BNC female connector that provides access to an analogue voltage proportional to the received power at the ODU input. A voltmeter is attached to the RSSI connector to measure the voltage when aligning the antenna. For more information, see Step 6: Aligning antennas on page 6-100.
6	CMU connector	This connects the ODU to the CMU via an IF cable.

Further reading on the ODU

For more information on the ODU, refer to the following:

- Grounding and lightning protection on page 2-7 describes the grounding and lightning protection requirements of a PTP 800 installation, including the ODU.
- Ordering ODUs on page 2-69 lists the ODUs available for PTP 800 installations, with Cambium part numbers.
- ODU specifications on page 4-5 contains specifications of the ODU, such as dimensions, weight and environmental requirements.
- Coupler mounting kit specifications on page 4-15 contains specifications of the couplers that may be used to connect two ODUs to one antenna.
- Installing antennas and ODUs on page 5-5 describes how to install the antennas, ODUs and waveguide connections at each link end, either in a direct mount or remote mount configuration, with or without couplers.

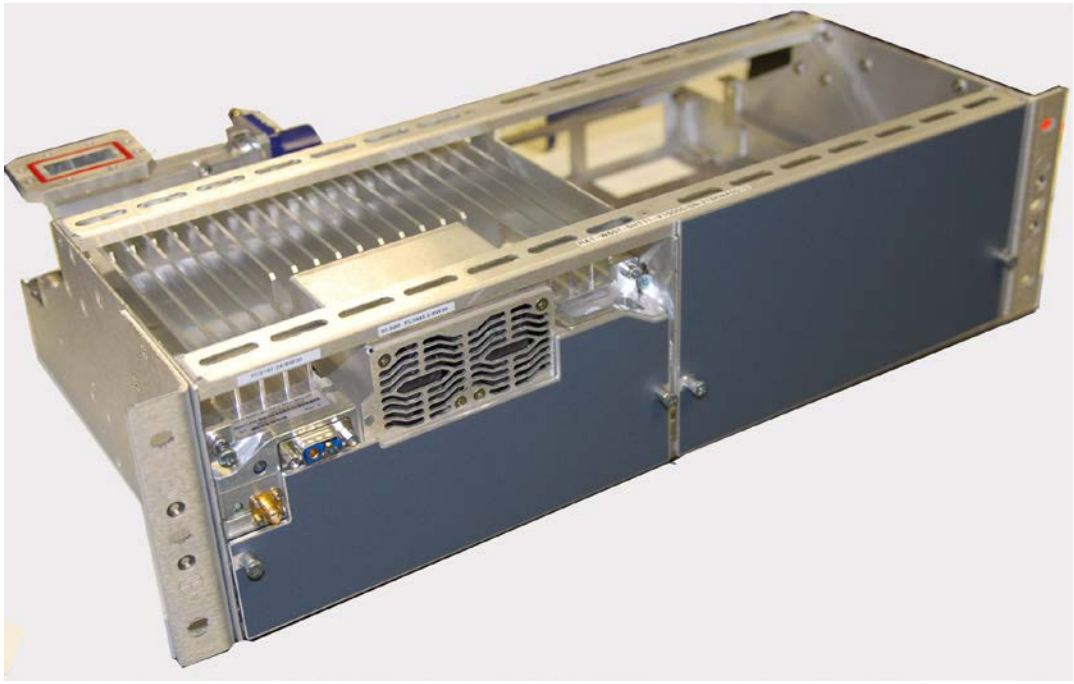
Indoor RF unit (IRFU)

This section describes the PTP 800 IRFU and its interfaces.

IRFU description

The PTP 800 indoor RF unit (IRFU) (Figure 10) converts signals between a modulated intermediate frequency (IF) and radio band frequencies for transmission over a line-of-sight link. The IRFU can be chosen as an alternative to the ODU to operate with one or two PTP 800 CMUs.

Figure 10 Top and front view of IRFU shelf (with single transceiver and waveguide)



The PTP 800 IRFU platform supports the licensed bands and frequencies listed in Table 3.

The IRFU chassis is designed for mounting in an indoor 19" rack. The 2.77 U height chassis can house one or two field replaceable transceivers, where each transceiver interfaces to a separate CMU via an intermediate frequency coaxial cable, or IF cable. The IRFU also provides either one or two waveguide interfaces for connection to the antenna or antennas. The waveguide interfaces have excellent voltage standing wave ratio (VSWR). This reduces the amplitude of reflected signals passing up the waveguide which could otherwise degrade the quality of the transmitted and received signals. When connected to a suitably low VSWR antenna, this makes the IRFU ideal for operation with a wide range of waveguide lengths.

Transceivers

Each transceiver provides the necessary frequency conversion and amplification of signals which pass between the CMU and antenna. In the transmit direction, a transceiver up-converts and amplifies the fixed intermediate frequency (IF) signal received from the CMU resulting in a configured licensed band radio frequency signal transmitted at the waveguide interface. In the receive direction, a transceiver provides low noise amplification and down-conversion of the licensed band signal received at the waveguide interface. The result is a fixed IF signal which is passed to the CMU for demodulation.

Each transceiver is powered via its own dedicated power socket. Cambium Networks do not provide the power supply, but they do provide the power connector. For power supply requirements, please see IRFU specifications on page 4-8.

NOTE

To prevent grounding issues with the CMU, only a -48 V dc power supply is supported.

Each transceiver is cooled by its own field replaceable fan assembly. Each fan assembly contains two fans which are automatically controlled by the transceiver which responds to changes in the temperature of its power amplifier.

As an aid to aligning antennas, the IRFU provides an interface per transceiver for monitoring the strength of the received signal level.

Branching unit

The transceivers connect to the waveguide interfaces via the IRFU branching unit. The branching unit is an integral part of the IRFU and is situated at the back of the chassis. The branching unit provides the necessary coupling and filtering and also the necessary isolation between transceivers. Although the branching unit is not field replaceable, the transmit and receive filters within the branching unit are both field replaceable.

IRFU availability

IRFUs are available at 6 GHz and 11 GHz. The 6 GHz IRFU support the L6 and U6 bands of both FCC and Industry Canada regulations. The FCC 7 GHz band is also supported by this IRFU. The 11 GHz IRFU supports the 11 GHz band for both FCC and Industry Canada regulations.

Although the transceivers are designed to cover the entire frequency range of a given band, the branching unit is factory tuned for a specific transmit frequency and a specific receive frequency. The transmit frequency and receive frequency must therefore be specified when ordering an IRFU.

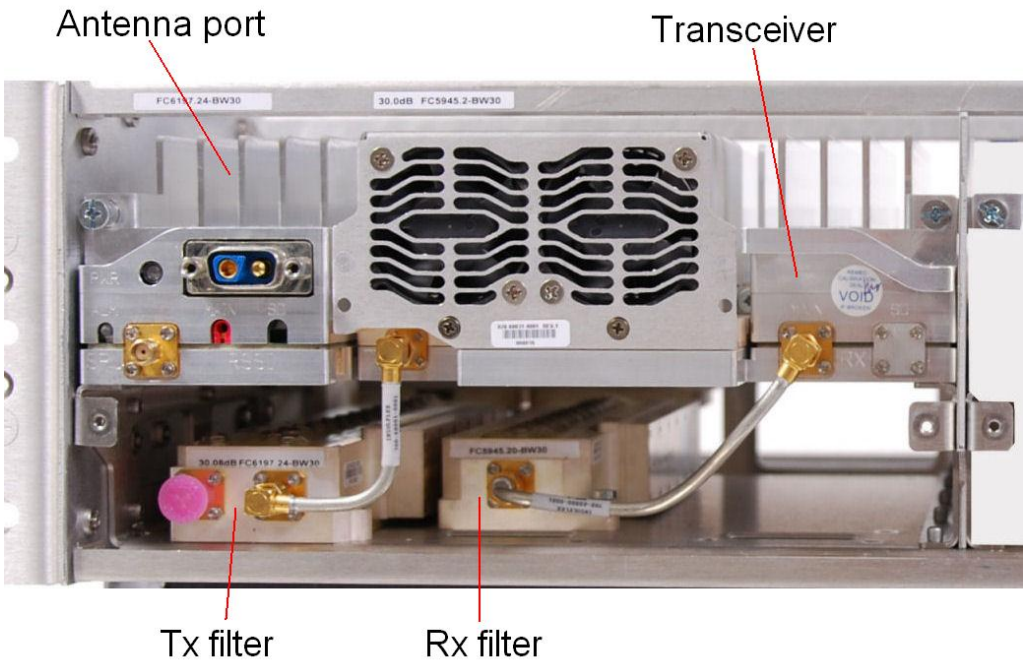
IRFU configuration options

IRFUs are available with the following optional configurations:

1+0

This consists of a single transceiver with the branching unit providing a single waveguide interface (Figure 11). With this option, the right hand transceiver position is not populated.

Figure 11 IRFU 1+0 configuration



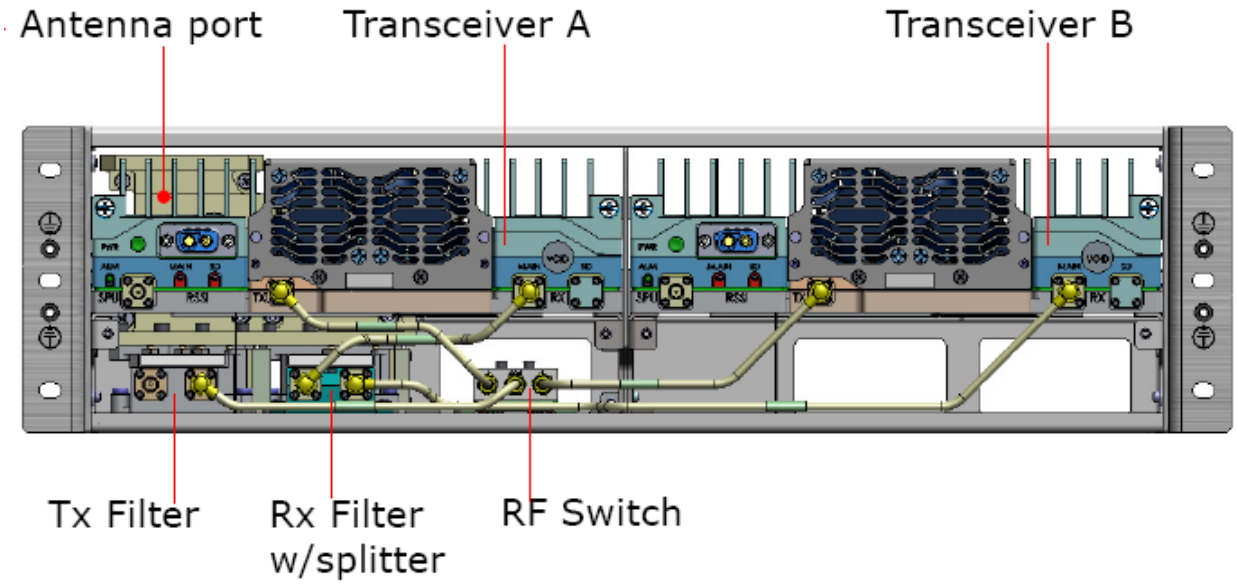
Back view:



1+1 Tx MHSB (with equal or unequal receiver coupling)

This option consists of two transceivers with the branching unit providing a single waveguide interface for connection to an antenna (Figure 12). This option provides monitored hot standby (MHSB) operation, which allows the link to continue to operate in the event of single point equipment failure. Both transceivers are capable of receiving and transmitting, but the transmission from only one of the transceivers is routed to the waveguide interface at any one time. This is achieved with an RF switch which is an integral component of the IRFU. The other transceiver remains on standby waiting to take over in case of equipment failure. This option is available with equal or unequal receive coupling, the latter providing a better radio link budget for the primary transceiver, which is the preferred transceiver. For more details of 1+1 operation, see 1+1 Hot Standby link protection on page 1-64.

Figure 12 IRFU 1+1 Tx MHSB configuration



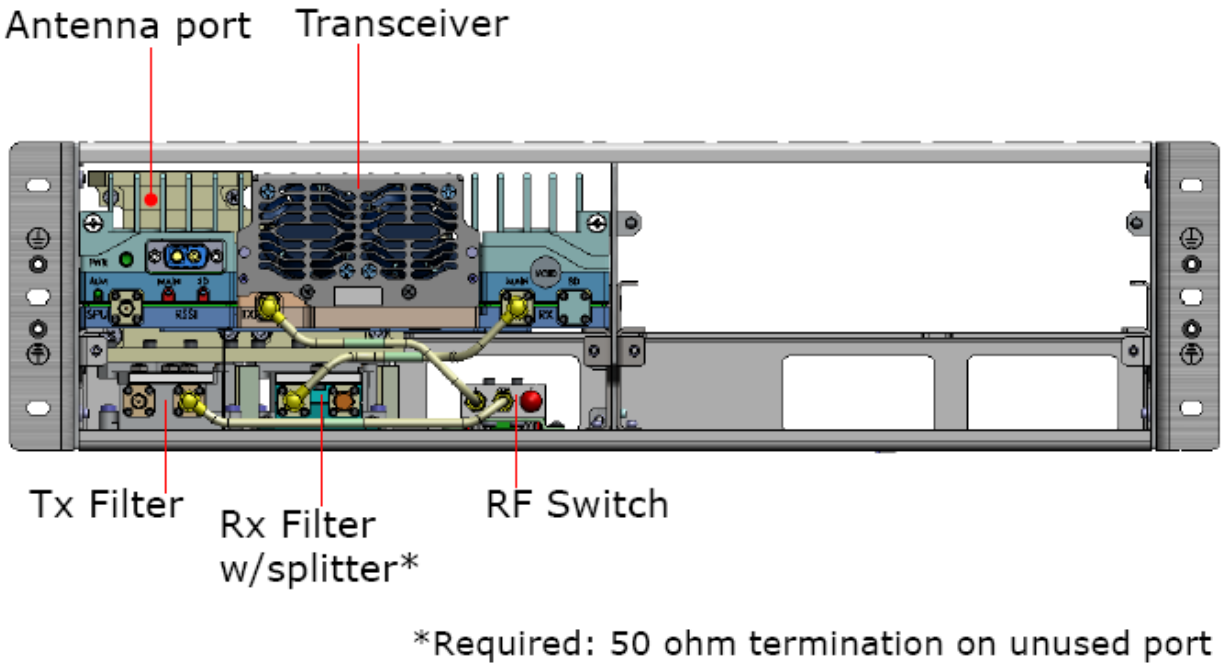
Back view:



1+0 Tx MHSB Ready (with equal or unequal receiver coupling)

This option consists of a single transceiver and a single waveguide interface (Figure 13), but the branching unit is ready for connection of a second transceiver if an upgrade to a full 1+1 Tx MHSB is required at a later date. Similar to the 1+1 Tx MHSB, this option is available with equal or unequal receive coupling.

Figure 13 IRFU 1+0 Tx MHSB Ready configuration



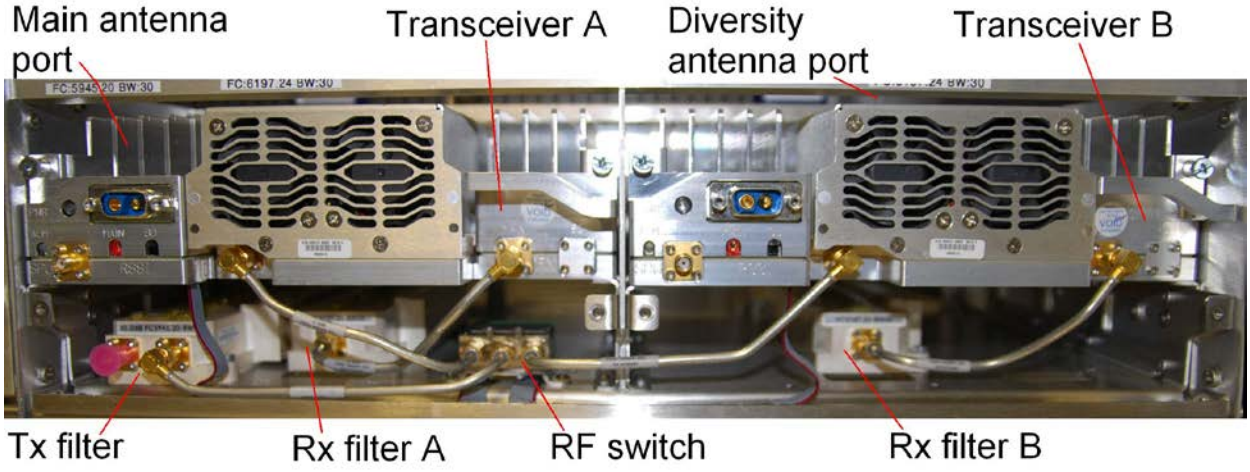
Back view:

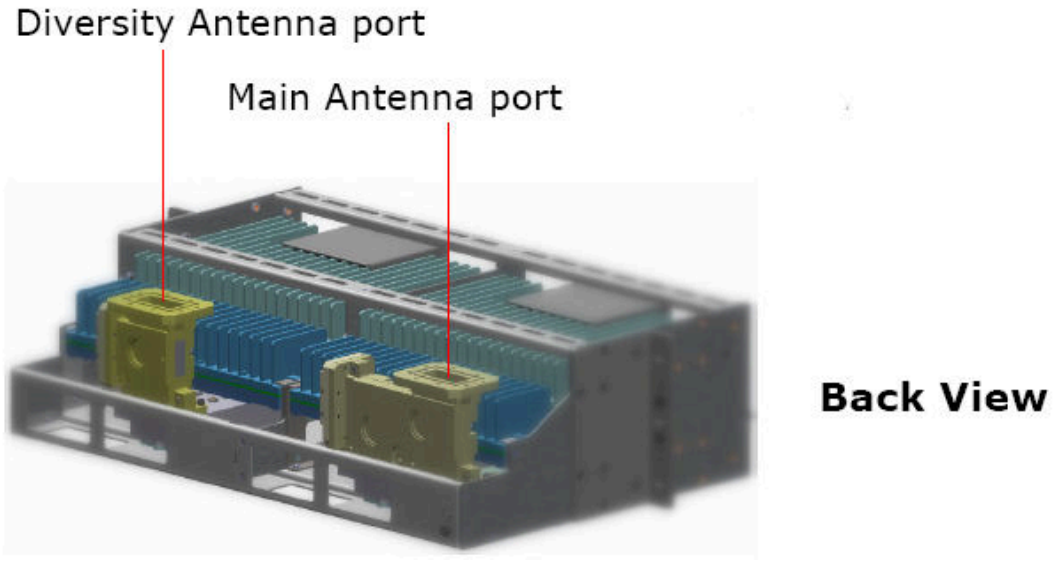


1+1 Tx MHSB / Rx SD

This option consists of two transceivers with the branching unit providing two waveguide interfaces (Figure 14). As well as providing MHSB operation in the event of single point equipment failure, it also provides Receive Spatial Diversity by providing a second waveguide interface which connects to a diverse antenna. The IRFU will only radiate from the main waveguide interface (left hand viewed from the front). Although both transceivers are capable of transmitting, the transmission from only one of the transceivers is routed to the main waveguide interface at any one time. This is achieved with an RF switch incorporated within the IRFU. In the receive direction, the left hand transceiver will receive from the left hand (or main) waveguide interface and the right hand transceiver will receive from the right hand (or diverse) waveguide interface.

Figure 14 IRFU 1+1 Tx MHSB / Rx SD configuration

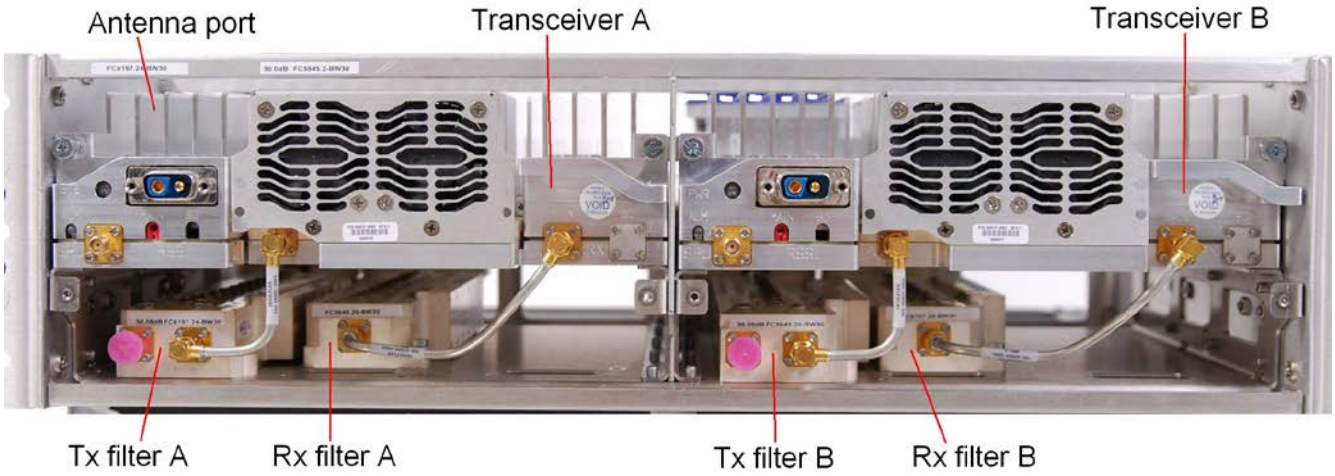


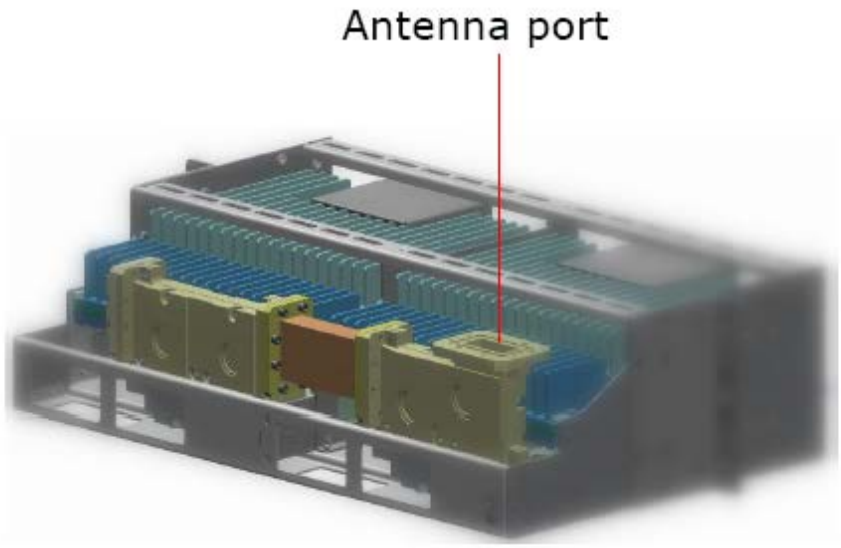


2+0

This option consists of two transceivers with the branching unit providing a single waveguide interface (Figure 15). This option provides two parallel 1+0 links which share the same antenna. Both transceivers will simultaneously transmit and receive through the same waveguide interface. Each transceiver must operate on a different transmit frequency and on a different receive frequency. A license will generally be required for each link.

Figure 15 IRFU 2+0 configuration





IRFU interfaces

The IRFU transceiver interfaces are illustrated in Figure 16 and described in Table 7.

Figure 16 IRFU transceiver interfaces

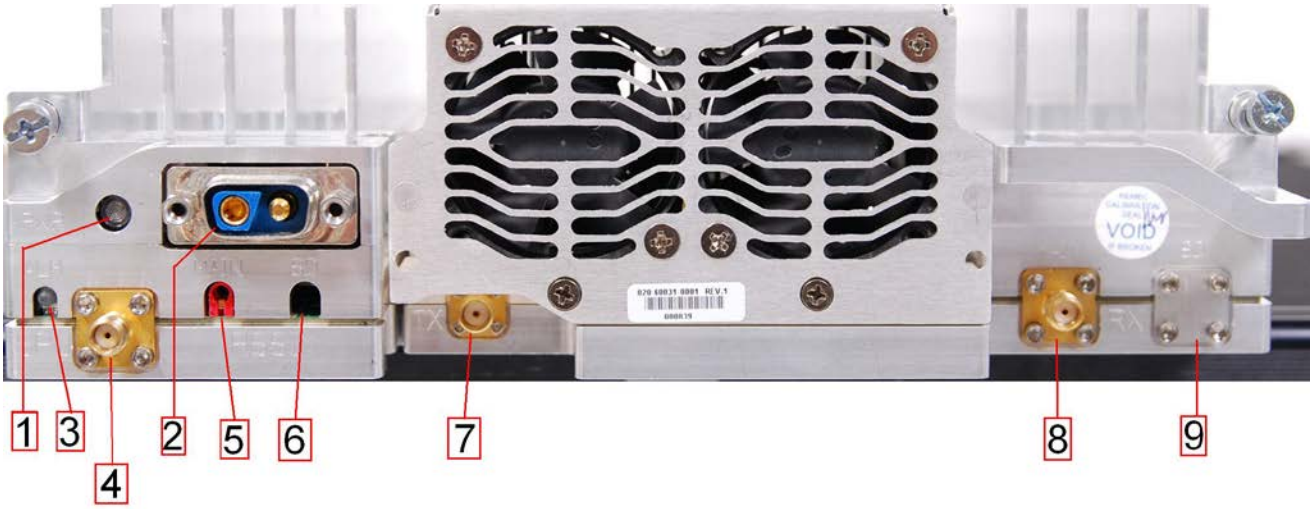


Table 7 IRFU transceiver interfaces

#	Interface	Function
1	Power button	For powering the transceiver on and off.
2	Power connector	For connecting the transceiver to a standard –48 V dc telecommunications supply.
3	“Alarm” LED	For indicating the status of the IRFU. LED states and troubleshooting actions are described in Check IRFU status LEDs on page 8-12.
4	CMU connector	For connecting the transceiver to the CMU via an IF cable with SMA connectors.
5	RSSI MAIN Test Jack	For connecting a voltmeter to measure the voltage when aligning the antenna. For more information, see Step 6: Aligning antennas on page 6-100.
6	RSSI SD Test Jack	As RSSI MAIN Test Jack, but measures the voltage when aligning the diversity antenna in 1+1 Tx MHSB / Rx SD configurations. Not equipped on single RX configurations.
7	TX Connector	For connecting the transceiver (transmit) to the BU via an RF cable with SMA connectors.

#	Interface	Function
8	RX Connector	For connecting the transceiver (receive) to the BU via an RF cable with SMA connectors.
9	RX SD Connector	For connecting the transceiver (receive diversity) to the BU via an RF cable with SMA connectors. Not equipped on single RX configurations.

Further reading on the IRFU

For more information on the IRFU, refer to the following:

- Grounding and lightning protection on page 2-7 describes the grounding and lightning protection requirements of a PTP 800 installation, including the ODU.
- Ordering IRFUs and accessories on page 2-91 lists the IRFUs, IRFU components, waveguides, antennas and antenna accessories for IRFU deployments, with Cambium part numbers.
- IRFU specifications on page 4-8 contains specifications of the IRFU, such as dimensions, weight, electrical and environmental requirements.
- Installing antennas and IRFUs on page 5-70 describes how to install an IRFU with antenna and waveguide.
- Replacing IRFU components on page 5-95 describes how to replaces IRFU components in operational links.

Antennas and couplers

This section describes the PTP 800 antennas, couplers and remote mounting kit.

Antennas

A typical antenna is shown in Figure 17.

Figure 17 Typical PTP 800 antenna with ODU (Cambium direct mount interface)



Antenna diameter

In each band, the antennas are provided in a number of diameters, the larger the diameter, the greater the gain.

Antenna interface

There are two types of antennas providing different interfaces to the RFU:

- **Direct mount interface**: The ODU mounts directly to the back of the antenna (Figure 18) and is secured using the integral spring loaded latches (Figure 19). Direct mount antennas are not installed with IRFUs.
- **Waveguide interface**: The antenna connects to the RFU via a waveguide (Figure 20). The RFU (ODU or IRFU) is mounted separately from the antenna.

Figure 18 Direct mount mechanical interface

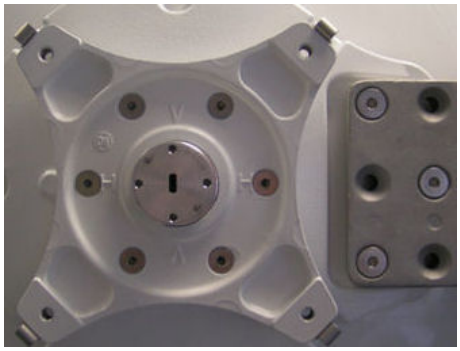


Figure 19 ODU clipped onto direct mount mechanical interface



Figure 20 Remote mount antenna waveguide interface



Antenna polarization

Antennas can be provided as single polar or dual polar:

- **Single polar** : A single polar antenna provides a single interface to the RFU. The antennas are normally supplied with vertical polarization. For horizontal polarization, the antennas can be modified by the user using the instructions provided. Single polar antennas can be provided with a direct mount interface or a waveguide interface.
- **Dual polar**: Dual polar antennas provide two interfaces, one with vertical polarization and one with horizontal polarization. This allows two links connecting the same two sites to share antennas, the two links operating on opposite polarizations. Dual Polar antennas provide a waveguide interface only.

Remote mounting kits (RMKs)

> **NOTE**
> Applies to ODU deployments only.

An RMK is used in an ODU (not IRFU) remote mount configurations to connect the ODU (or coupler) to the antenna via a flexible waveguide. Direct mount configurations do not require RMKs. The RMK has the following features:

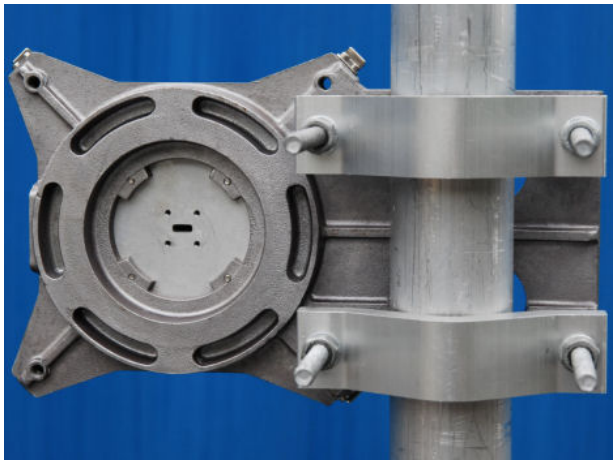
- A clamp for attaching the RMK to a monopole.
- A cylindrical transition (Figure 21) onto which the ODU mounts.
- A waveguide interface transition (Figure 22) for connection to the antenna via a flexible waveguide.

The choice of RMK depends upon the frequency variant. The 11 GHz RMK is always used with a tapered transition between the antenna and the flexible waveguide.

Figure 21 RMK showing the ODU interface



Figure 22 RMK showing the waveguide interface



Coupler mounting kits

> **NOTE**
> Applies to ODU deployments only.

The signals from two ODUs can be coupled to a single antenna. The ODUs mount directly to the coupler (Figure 23) which then provides an interface to the antenna which is identical to that of an ODU. The coupler can mount directly to the back of a direct mount interface antenna (Figure 24), or it can be mounted separately using the remote mounting kit (RMK).

Coupler mounting kits are provided in two options:

- **Symmetric coupler mounting kits**: This option splits the power evenly between the two ODUs. A nominal 3 dB is lost in each arm of the coupler.
- **Asymmetric coupler mounting kits** : This option splits the power in a way which favours one ODU. A nominal 1 dB is lost in the Main arm of the coupler with a nominal 7 dB being lost in the other arm. This is often a preferred option for 1+1 Hot Standby links (see Link types on page 1-6).

> **NOTE**
> Couplers increase system loss.

The choice of coupler mounting kit depends on the frequency variant and on the coupler type required (symmetric or asymmetric).

Figure 23 ODU coupler mounting kit



Figure 24 Two ODUs and antenna mounted on a coupler



Direct mount dual-polar antennas

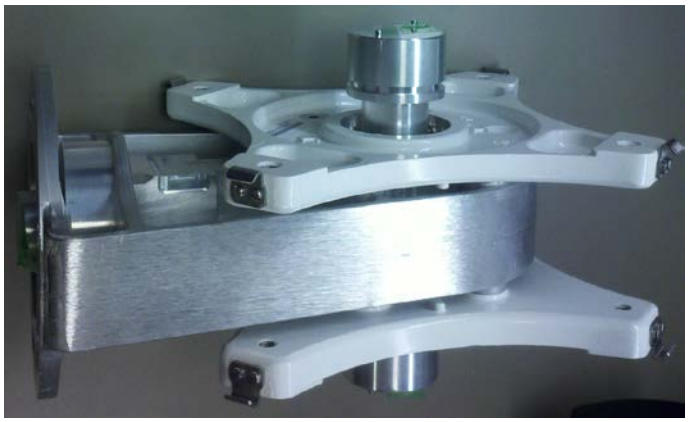
> **NOTE**
> Applies to ODU deployments only.

Direct mount dual-polar antennas are only used in 2+0 cross-polar direct mount configurations. They are supplied with an orthogonal mode transducer (Figure 25) with transitions (vertical and horizontal) that allow two ODUs to be coupled to the antenna.

Cambium supply dual-polar direct mount antennas as listed in Ordering antennas on page 2-59.

However, if a previously purchased antenna is to be upgraded to support a 2+0 cross-polar direct mount configuration, Cambium can supply separate orthogonal mount kits (OMKs), as listed in Ordering OMKs on page 2-90. The OMK can only be fitted to an antenna that is in the same band, for example, a 6 GHz antenna can only accept a 6 GHz OMK.

Figure 25 Orthogonal mode transducer



Further reading on antennas and couplers

For more information on antennas and antenna accessories, refer to the following:

- Site selection on page 2-3 describes how to select a site for the antenna.
- Grounding and lightning protection on page 2-7 describes the grounding and lightning protection requirements of a PTP 800 installation, including the antenna.
- Ordering antennas on page 2-59 lists the antennas required for PTP 800 installations, with Cambium part numbers.
- Ordering RMKs and waveguides on page 2-85 lists the RMKs, waveguides, hangers and transitions required for PTP 800 installations, with Cambium part numbers.
- Ordering coupler mounting kits on page 2-88 lists the couplers required for PTP 800 installations, with Cambium part numbers.
- Ordering OMKs on page 2-90 lists the OMKs required for PTP 800 installations, with Cambium part numbers.
- Equipment specifications on page 4-2 contains specifications of the flexible waveguides and couplers.
- Installing antennas and ODUs on page 5-5 describes how to install the antennas, ODUs and waveguide connections at each link end, either in a direct mount or remote mount configuration, with or without couplers.
- Task 12: Aligning antennas on page 6-98 describes how to align the two antenna in a link.

Cabling and lightning protection

This section describes the cabling and lightning protection components of a PTP 800 installation.

Lightning protection (ODU platforms only)

The PTP 800 has been tested for compliance to the EMC immunity specifications identified in EMC immunity compliance on page 4-82.

The ODUs for the PTP 800 are fitted with surge limiting circuits and other features to minimize the risk of damage due to nearby lightning strikes. To be fully effective, these standard features require some additional equipment to be configured as part of the system installation.

⚠ CAUTION

The PTP 800 Series is not designed to survive direct lightning strikes. For this reason the antenna and ODU should not be installed at the highest point in a localized area. See Grounding and lightning protection on page 2-7.

RFU to CMU connections

The RFU is connected to the LPUs and CMU using CNT-400 coaxial cable (IF cable).

CMU to network connections

The CMU is connected to network equipment using either a copper data port (100baseT or 1000baseT Ethernet) or a fiber interface (1000BaseSX or 1000BaseLX).

Cable grounding (ODU platforms only)

The ODU, LPUs and IF cable must be grounded to the supporting structure at the points specified in Grounding and lightning protection on page 2-7. One cable grounding kit (Figure 26) is required at each grounding point.

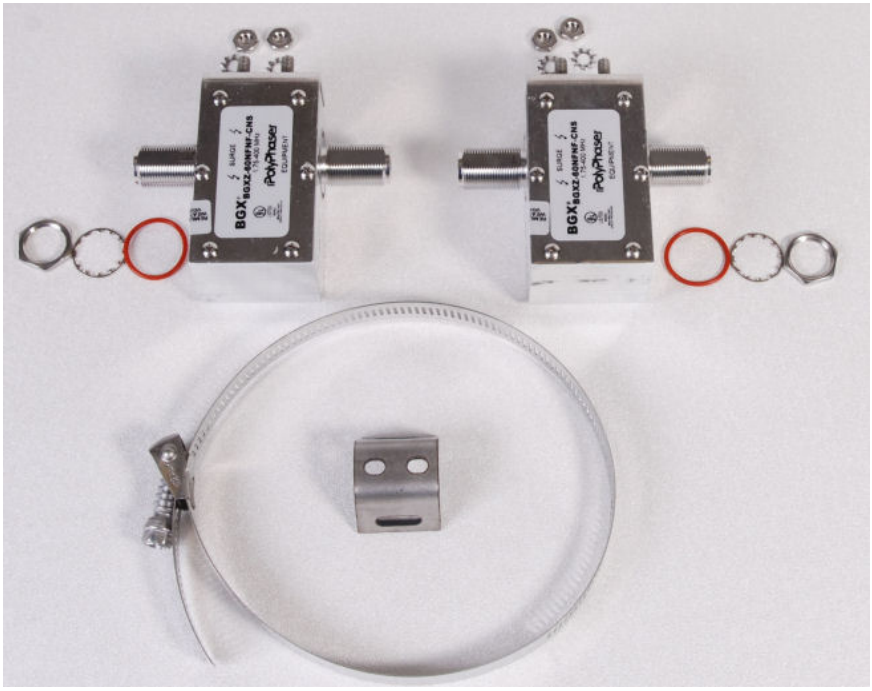
Figure 26 Cable grounding kit for 1/4" and 3/8" cable



Lightning protection units (LPUs)

The PTP 800 LPU end kit (Figure 27) is required for IF cables. One LPU is installed next to the ODU and the other is installed near the building entry point.

Figure 27 PTP 800 LPU end kit



Further reading on cabling and lightning protection

For more information on cabling and lightning protection, refer to the following:

- Maximum IF cable length on page 2-3 gives the maximum permitted lengths of IF cables in PTP 800 installations.
- Grounding and lightning protection on page 2-7 describes the grounding and lightning protection requirements of a PTP 800 installation.
- Ordering IF cable, grounding and LPUs on page 2-80 lists the cables, connectors, grounding kits and LPUs required for PTP 800 installations.
- Installing the IF and ground cables on page 5-36 describes how to install the IF cables and how to install grounding and lightning protection.

Wireless operation

This section describes how the PTP 800 wireless link is operated, including modulation modes, power control and security.

Channel separation

The PTP 800 wireless link supports the following channel separations:

- 7 MHz
- 13.75 MHz
- 14 MHz
- 27.5 MHz
- 28 MHz
- 29.65 MHz
- 30 MHz
- 40 MHz
- 55 MHz
- 56 MHz
- 60 MHz

The available selection of channel separations varies depending on band and region.

Channel bandwidth

The PTP 800 wireless link supports the following channel bandwidths:

- 10 MHz
- 20 MHz
- 25 MHz
- 30 MHz
- 40 MHz
- 50 MHz
- 80 MHz.

The available selection of channel bandwidths varies depending on band and region.

Modulation modes

The PTP 800 wireless link operates using single carrier modulation with the following fixed modulation modes:

- QPSK
- 8PSK
- 16QAM
- 32QAM
- 64QAM
- 128QAM
- 256QAM

The available selection of modulation modes varies depending on band, region and channel bandwidth.

PTP 800 uses Low Density Parity Check (LDPC) forward error correction (FEC) coding. The code rate is calculated as the ratio between the un-coded block size and the coded block size. FEC code rate in PTP 800 varies between 0.76 and 0.94 depending on channel bandwidth and modulation mode.

For more information, see Capacity, transmit power and sensitivity on page 4-22.

Adaptive coding and modulation

PTP 800 supports both Fixed Modulation and Adaptive Coding and Modulation (ACM) modes. In ACM mode, the PTP 800 selects the modulation mode according to the quality of the received signal. The selection criterion is to provide the highest link capacity that can be achieved while keeping the communication error free.

When compared with Fixed Modulation operation, ACM can increase either link availability, or average wireless link capacity, or both.

> **NOTE**
> ODU-B offers superior ACM characteristics to ODU-A.

Automatic transmitter power control

PTP 800 provides closed-loop automatic transmitter power control (ATPC). ATPC avoids overload of the receivers in links with low link loss by automatically adjusting transmitter power. The ATPC threshold is –40 dBm received power. ATPC has no effect in links where the received power is lower than the threshold.

Automatic adjustment of the transmitter can be enabled or disabled using the Automatic Transmitter Power Control attribute on the Configuration page of the web-based interface. This attribute must have the same setting at both ends of the link.

In some regions ATPC is a regulatory requirement and in these cases ATPC cannot be disabled.

The power control loop compensates for slow variations in received power and does not respond to fast fading that occurs in multipath channels.

In addition to its main function, ATPC includes a mechanism protecting against a lock up scenario. The mechanism is active regardless of the received power. This lock up occurs when the configured maximum transmit power causes the received power at both ends of the link to be too high to allow correct signal demodulation. In this situation, no communication can be established in either direction, causing the radios to wait forever for the remote end to appear.

The protection mechanism works as follows. Upon the link dropping for more than 10 seconds, ATPC drops the maximum transmit power of the end which has the lowest transmit frequency by 15 dB. This ensures the link will come up even if the maximum transmit power is set incorrectly. The delay prevents this mechanism from being triggered when the link drops briefly due to severe fading.

Maximum receive power

The maximum receive power is the maximum power at which a PTP 800 link should be operated to maintain error free communication. This maximum receive power for normal operation is -35 dBm. Automatic transmitter power control, if enabled, will reduce the installation receive level to a -40 dBm operating level if there is sufficient dynamic range available in the maximum transmit power. For example, a link installed at -35 dBm with a maximum transmit power set to at least 5 dB above the minimum power level will successfully operate at -40 dBm. Links operating without ATPC, or with less than 5 dB available dynamic range should ensure that the normal operating level does not exceed -35 dBm.

On very short links it may be necessary to use a fixed waveguide attenuator, which will require the use of a remote mount antenna, to keep the maximum receive power at an acceptable level.

Maximum transmit power

Maximum transmit power is the maximum power that the PTP 800 is permitted to generate at the waveguide interface assuming that ATPC is disabled, or the link loss is high enough such that ATPC is not activated. The equipment limit for maximum transmit power is defined by modulation mode, band, channel bandwidth and standards body or region. The spectrum license limit is determined by the maximum EIRP permitted by the individual license, the antenna gain and feeder loss. The maximum transmit power that can be configured for PTP 800 is limited by the more restrictive of the equipment limit and the spectrum license limit.

Maximum transmit power defaults to the maximum permitted as described above, but can be reduced if necessary using Step 3 of the Installation Wizard, or the Configuration page of the web-based interface.

Security

PTP 800 provides optional 128-bit and 256-bit encryption using the Advanced Encryption Standard (AES). The implementation in PTP 800 has been validated against Federal Information Processing Standard Publication 197 (FIPS-197) in the Cryptographic Algorithm Validation Program (CAVP) of the US National Institute of Standards and Technology (NIST).

AES encryption protects all traffic over the wireless link, including in-band and out-of-band network management traffic. Each CMU behaves as a cryptographic device in which the Ethernet interfaces transmit and receive plain text data, and the IF interface transmits and receives cipher text data. The IF cable and RFUs are outside the cryptographic boundary.

Further reading on wireless operation

For more information on wireless operation, refer to the following:

- Link planning on page 2-2 describes factors to be taken into account when planning links, and introduces PTP LINKPlanner.
- Wireless specifications on page 4-19 contains specifications of the PTP 800 wireless interface, such as RF bands, channel width, spectrum settings, maximum power and sensitivity.
- Electromagnetic compliance on page 4-82 describes how the PTP 800 complies with the radio regulations that are in force in various countries.
- Task 7: Configuring wireless interface on page 6-63 describes how to configure the wireless interface using the installation wizard.

- Comparing actual to predicted performance on page 6-110 describes how to check that a newly installed link is achieving predicted levels of performance.
- Disabling and enabling the wireless interface on page 7-32 describes how to disable wireless transmission (prevent antenna radiation) and enable wireless transmission (allow antenna radiation).
- Managing performance on page 7-57 describes how to manage the performance of a PTP 800 link.

Ethernet bridging

This section describes how the PTP 800 controls Ethernet data, in both the customer data network and the system management network.

Customer network

Transparent Ethernet service

The PTP 800 Series provides an Ethernet service between the data port at a local CMU and the data port at an associated remote CMU. The Ethernet service is based on conventional layer two transparent bridging, and is equivalent to the Ethernet Private Line (EPL) service defined by the Metro Ethernet Forum (MEF).

The service is transparent to untagged frames, standard VLAN frames, priority-tagged frames, provider bridged frames, and provider backbone bridged frames. In each case, the service preserves MAC addresses, VLAN ID, Ethernet priority and Ethernet payload in the forwarded frame. The maximum frame size for bridged frames in the customer network is 9600 octets.

Layer two control protocols

The PTP 800 Series is transparent to layer two control protocols (L2CP) including:

- Spanning tree protocol (STP), rapid spanning tree protocol (RSTP)
- Multiple spanning tree protocol (MSTP)
- Link aggregation control protocol (LACP)
- Link OAM, IEEE 802.3ah
- Port authentication, IEEE 802.1X
- Ethernet local management interface (E-LMI), ITU-T Q.933.
- Link layer discovery protocol (LLDP)
- Multiple registration protocol (MRP)
- Generic attribute registration protocol (GARP)

PTP 800 handles IEEE 802.3 Pause frames as a special case; each CMU can be configured to either forward (tunnel) or discard Pause frames received at the Data port. PTP 800 discards all Pause frames received at the Management port.

The PTP 800 Series does not generate or respond to any L2CP traffic.

Quality of service for bridged Ethernet traffic

The PTP 800 Series supports eight traffic queues for Ethernet frames waiting for transmission over the wireless link. Ethernet frames are classified by inspection of the Ethernet destination address, the Ethernet priority code point in the outermost VLAN tag, the Differentiated Services Code Point (DSCP) in an IPv4 or IPv6 header, or the Traffic Class in an MPLS header.

PTP 800 provides a configurable mapping between Ethernet, IP or MPLS priority and transmission queue, together with a simple way to restore a default mapping based on the recommended default in IEEE 802.1Q-2005. Untagged frames, or frames with an unknown network layer protocol, can be separately classified.

Scheduling for transmission over the wireless link is by strict priority. In other words, a frame at the head of a given queue is transmitted only when all higher priority queues are empty.

Fragmentation

The PTP 800 Series minimizes latency and jitter for high-priority Ethernet traffic by fragmenting Ethernet frames before transmission over the wireless link. The fragment size is selected automatically according to channel bandwidth and modulation mode of the wireless link. Fragments are reassembled on reception, and incomplete Ethernet frames are discarded. Traffic is not fragmented in the highest priority traffic class.

Management network

IP interface

Each PTP 800 CMU contains an embedded management agent with a single IP interface. Network management communication is exclusively based on IP and associated higher layer transport and application protocols. The default IP address of the management agent is 169.254.1.1. The PTP 800 does not require use of supplementary serial interfaces.

In a 1+1 protection scheme, each CMU contains a separate management agent.

MAC address

The management agent end-station MAC address is recorded on the underside of the enclosure. The MAC address is not configurable by the user.

VLAN membership

The management agent can be configured to transmit and receive either untagged, priority-tagged, C-tagged (IEEE 802.1Q) or S-tagged (IEEE 801.ad) frames. S-tagged frames must be single tagged, in other words, an S-tag with no encapsulated C-tag. The VLAN ID can be 0 (priority tagged) or in the range 1 to 4094.

Out-of-band management

PTP 800 supports an end-to-end out-of-band management mode in which the management agent can be reached from the management port at the local CMU, and (assuming that the wireless link is established) the management port at the remote CMU. This management mode allows communication from the CMU management port to Ethernet end stations reached through the remote CMU, supporting construction of an extended management network that is isolated from the customer network.

End-to-end out-of-band management is possible only when the network management mode is configured to “out-of-band” at every CMU.

Out-of-band quality of service

Out-of-band management traffic is forwarded over the wireless link using a dedicated channel. The management channel represents a single traffic class, and the same quality of service is afforded to all management frames. Traffic in the management channel is fragmented for transmission over the wireless link to minimize the jitter imposed on high priority traffic in the customer network.

The management channel has higher priority than traffic in the customer network, subject to a configurable committed information rate (CIR) with a range between 200 Kbit/s and 2 Mbps. Committed capacity that remains unused by management traffic is available for customer traffic.

Out-of-band local management

The out-of-band local management mode is similar to the standard out-of-band mode, except that management frames are not forwarded over the wireless link. Connection to the management agent is solely through the management port of the local CMU. The management channel CIR control is disabled in out-of-band local mode.

Out-of-band local management is the default management mode.

If the management port is not accessible remotely, this mode should be changed to permit remote management.

In-band management

In the in-band management mode, the management agent can be reached from the data port at the local CMU, and (assuming that the wireless link is established) the data port at the remote CMU. In this mode, the management port is disabled.

Management frames in the customer network are processed by the management agent if (a) destination MAC address in the frame matches the CMU MAC address, and (b) the VLAN ID in the frame matches the VLAN configuration of the management agent.

If Local Packet Filtering is enabled, unicast frames forwarded to the management agent are filtered, that is, not forwarded in the customer network.

In-band quality of service

The CMU may be configured to tag the Ethernet frames generated by its management agent. When configured for In Band Management, these frames are assigned to a queue based on the priority code point in the same way as customer traffic.

Source address learning

If Local Packet Filtering is enabled, the management agent learns the location of end stations from the source addresses in received management frames. The agent filters transmitted management frames to ensure that the frame is transmitted at the Ethernet (data or management) port, or over the wireless link as appropriate. If the end station address is unknown, then management traffic is transmitted at the Ethernet port and over the wireless link.

In out-of-band local management mode, management frames are not transmitted over the wireless link, and so address learning is not active.

Wireless link down alert

The PTP 800 Series can be configured to alert a ‘loss of link’ to the connected network equipment. It does this by means of a brief disconnection of the copper data port or fiber data port. When the PTP 800 Series is configured for out-of-band operation, it also briefly disconnects the management port. Ethernet disconnection typically occurs within 50 ms of detection of link failure. The alert is triggered by any condition which prevents the link from forwarding traffic in one or both link directions. Examples include a deep wireless fade, equipment failure such as an RFU failure, and Ethernet cable disconnection. In 1+1 Hot Standby links, the alert will only be triggered if a protection switch does not resolve the failure condition, for example if both sets of equipment at an end exhibit a fault or if there is a deep wireless fade.

The wireless link down alert can be deployed in networks which provide alternative traffic routes in the event of failure. Spanning Tree Protocol (STP) and Ethernet Automatic Protection Switching (EAPS) are two protocols which are commonly deployed in such complex networks and both react to the wireless link down alert.

Protocol model

Ethernet bridging behavior at each end of the wireless link is equivalent to a three-port, managed, transparent MAC bridge where the three ports are:

- Ethernet Management Port
- Ethernet Data Port
- Wireless Port

Frames are transmitted at the Wireless port over a proprietary point-to-point circuit-mode link layer between ends of the PTP 800 link. For a single CMU configuration or the active CMU in a 1+1 Hot Standby configuration, Ethernet frames received at the data or management ports, or generated internally within the management agent, are encapsulated within a lightweight MAC layer for transmission over the wireless link.

For the inactive CMU at a protected end no traffic is transmitted over the wireless link. Any management traffic generated is transmitted towards the management port (for out-of-band management) or the traffic port (for in-band management).

Forwarding behavior

In out-of-band local mode (Figure 28) and out-of-band mode (Figure 29), the management network (shown in red) is isolated from the customer data network (shown in blue). In out-of-band mode, the management network is isolated from the customer data at the wireless port by use of a separate service access point and associated dedicated logical channel. Ethernet frames will not leak between management and data networks, even in the presence of configuration errors.

In in-band mode (Figure 30), the management and customer data networks are not isolated, and the Management port is not used.

Figure 28 Forwarding behavior in out-of-band local management mode

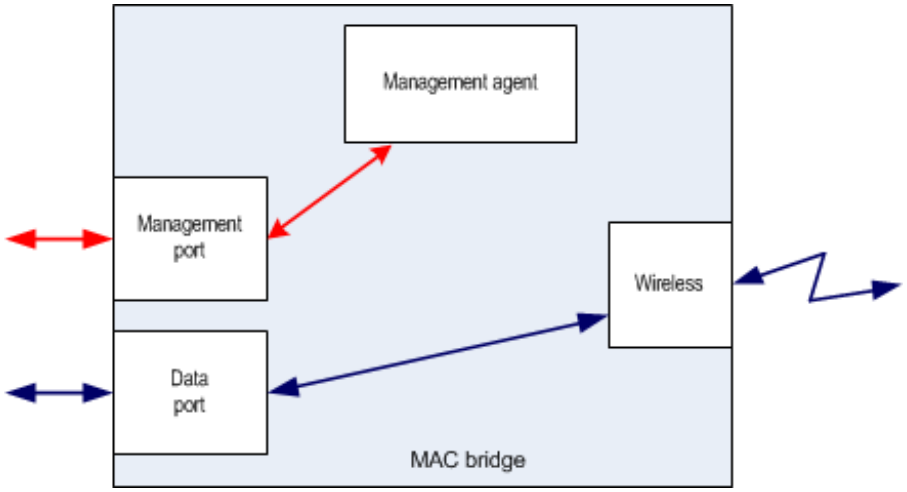


Figure 29 Forwarding behavior in out-of-band management mode

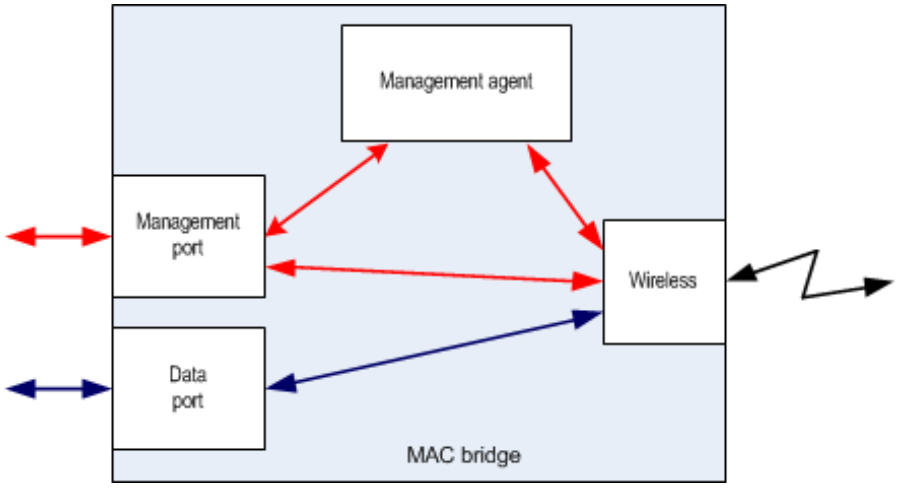
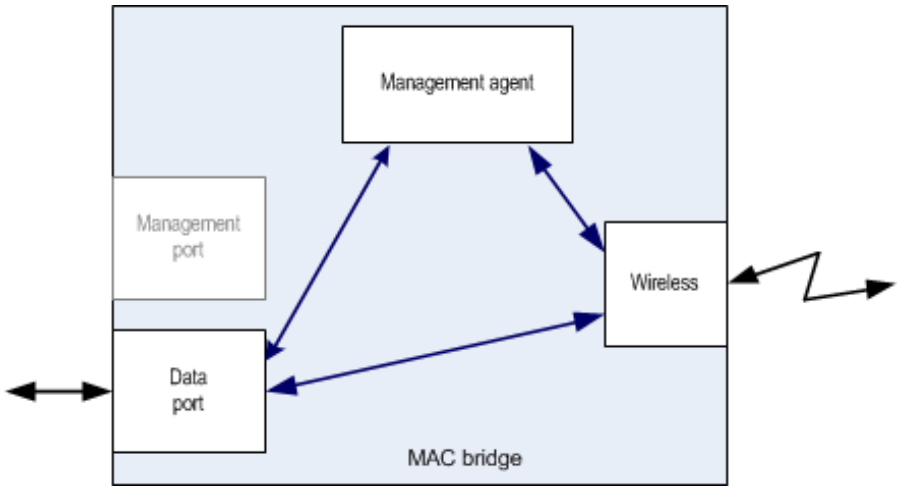


Figure 30 Forwarding behavior in in-band mode



Forwarding behavior for 1+1 Hot Standby links

Forwarding behavior for the active CMU is as for a non-protected link.

Forwarding behavior for the inactive CMU in a 1+1 Hot Standby link requires management data to be routed to the Ethernet management port (Figure 31) or data port (Figure 32), depending on the management mode. Only status information from the remote CMU is forwarded at the wireless interface.

Figure 31 Inactive unit frame forwarding – out-of-band management

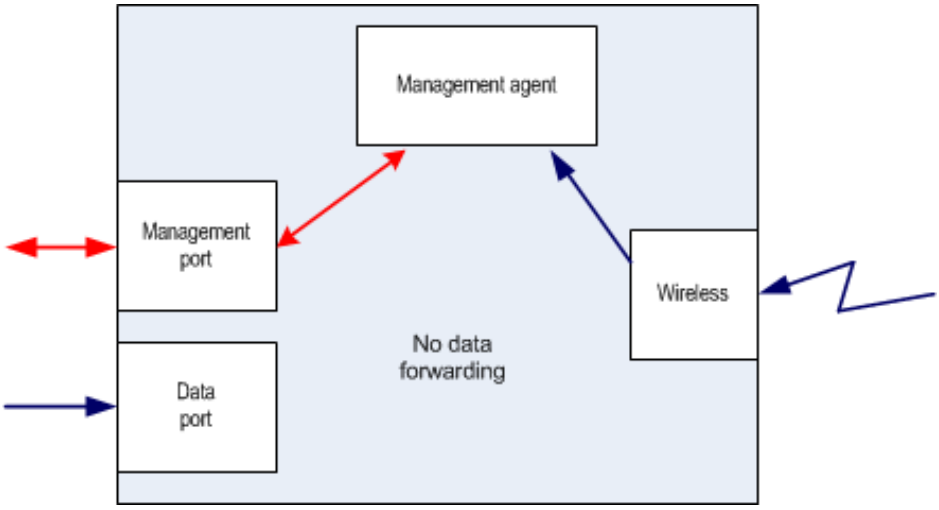
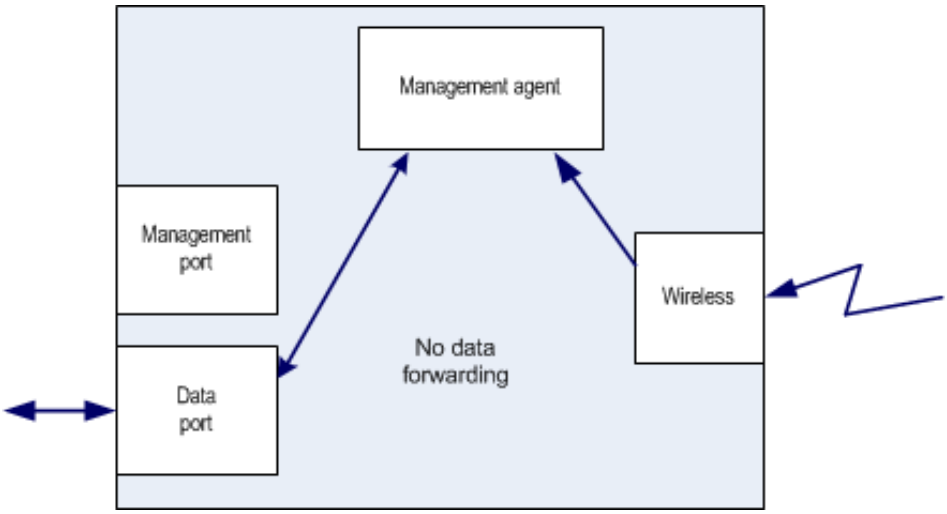


Figure 32 Inactive unit frame forwarding – in-band management



Protocol layers

Protocol layers involved in bridging between Ethernet and wireless interfaces are shown in Figure 33. Protocol layers involved in bridging between external interfaces and the management agent are shown in Figure 34. In these figures, the layers have the meanings defined in IEEE 802.1Q-2005.

Figure 33 Protocol layers between Ethernet and wireless interfaces

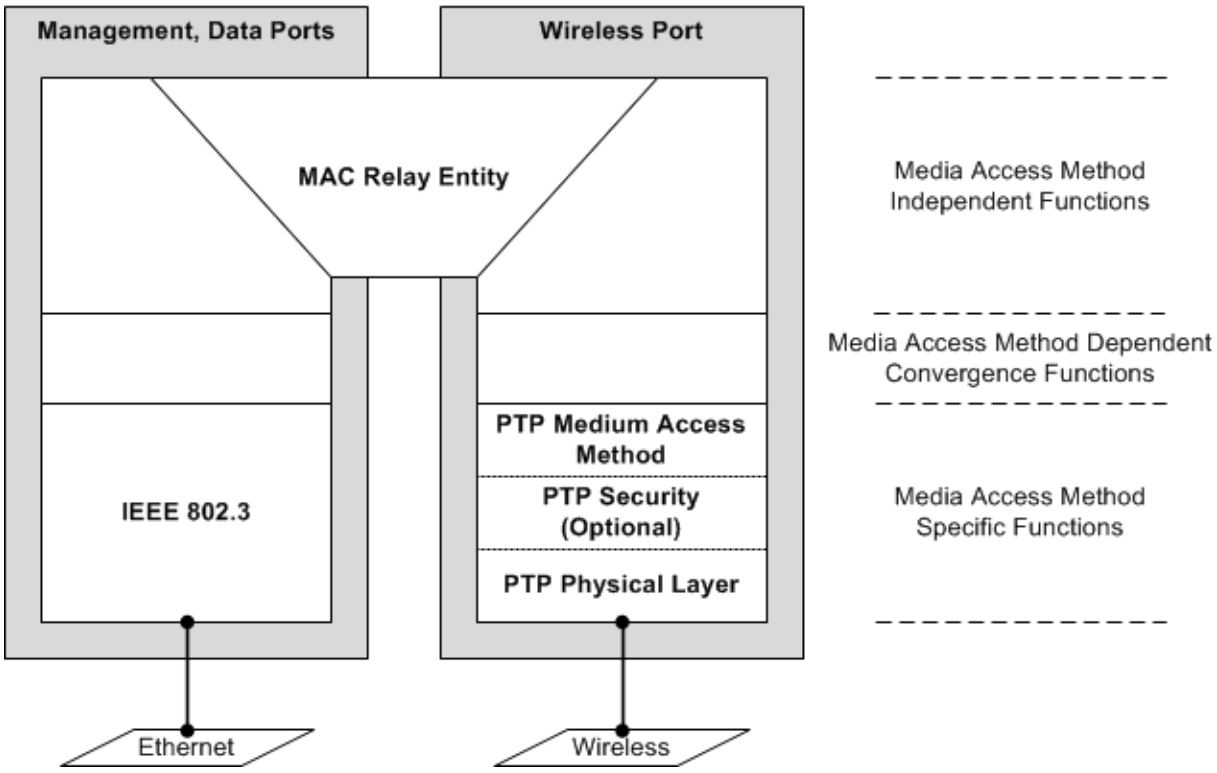
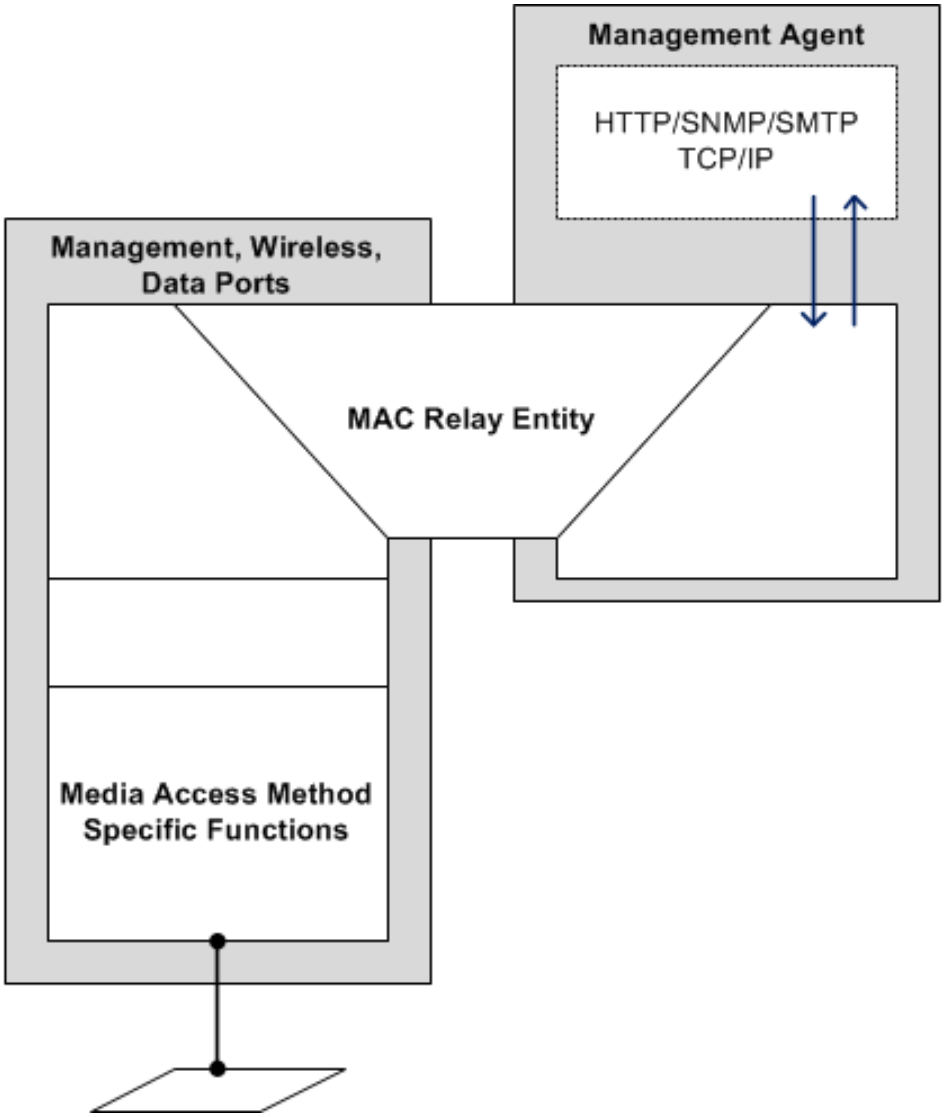


Figure 34 Protocol layers between external interfaces and the management agent



Further reading on Ethernet bridging

For more information on Ethernet bridging, refer to the following:

- Data network planning on page 2-18 describes factors to be considered when planning PTP 800 data networks.
- Data network specifications on page 4-71 contains specifications of the PTP 800 Ethernet interfaces.
- Task 2: Configuring IP and Ethernet interfaces on page 6-8 describes how to configure the IP and Ethernet attributes of the PTP 800.

System management

This section introduces the PTP 800 management system, including the web interface, installation, configuration, alerts and upgrades.

Management agent

PTP 800 equipment is managed through an embedded management agent. Management workstations, network management systems or PCs can be connected to this agent using an in-band mode, or a choice of two out-of-band modes. These modes are described in detail in Management network on page 1-43.

The management agent supports the following interfaces:

- Hyper text transfer protocol (HTTP)
- HTTP over transport layer security (HTTPS/TLS)
- RADIUS authentication
- Simple network management protocol (SNMP)
- Simple mail transfer protocol (SMTP)
- Simple network time protocol (SNTP)
- System logging (syslog)

Web server

The PTP 800 management agent contains a web server. The web server supports the HTTP and HTTPS/TLS interfaces.

Operation of HTTPS/TLS is enabled by purchase of an optional AES upgrade as described in Task 3: Installing license keys on page 6-21.

Web-based management offers a convenient way to manage the PTP 800 equipment from a locally connected computer or from a network management workstation connected through a management network, without requiring any special management software. The web-based interfaces are the only interfaces supported for system installation, and for the majority of configuration management tasks.

Transport layer security

The HTTPS/TLS interface provides the same set of web-pages as the HTTP interface, but allows HTTP traffic to be encrypted using Transport Layer Security (TLS). PTP 800 uses AES encryption for HTTPS/TLS.

HTTPS/TLS requires installation of a private key and a public key certificate where the common name of the subject in the public key certificate is the IP address or host name of the PTP 800 unit.

HTTPS/TLS operation is configured through the web-based interfaces using the Security Wizard.

Details of the security material needed for HTTPS/TLS are provided in Security planning on page 2-22.

> **NOTE**
> The PTP 800 has no default public key certificate, and Cambium is not able to generate private keys or public key certificates for specific network applications.

User account management

PTP 800 allows a network operator to configure a policy for login attempts, the period of validity of passwords and the action taken on expiry of passwords. See Configuring local user accounts on page 6-42 for further details.

Identity-based user accounts

The PTP 800 web-based interface provides two methods of authenticating users:

- Role-based user authentication allows the user, on entry of a valid password, to access all configuration capabilities and controls. This is the default method.
- Identity-based user authentication supports up to 10 users with individual usernames and passwords.

When identity-based user accounts are enabled, a security officer can define from one to ten user accounts, each of which may have one of the three possible roles:

- Security officer.
- System administrator.
- Read only.

Identity-based user accounts are enabled in the Local User Accounts page of the web-based interface.

Password complexity

PTP 800 allows a network operator to enforce a configurable policy for password complexity. Password complexity configuration additionally allows a pre-determined best practice configuration to be set. See Configuring local user accounts on page 6-42 for further details.

Installation wizard

The web-based interface includes an Installation wizard. This feature simplifies the process of entering initial configuration details, setting the system into alignment mode, achieving the lowest possible link loss through correct antenna alignment, and reporting on the performance of the installed link. The process handles the important configuration settings that must be set to comply with individual license conditions. These important settings are not normally modified in an operating link, and cannot be changed in PTP 800 except through use of the Installation wizard.

Configuration pages

The web-based interface includes a number of configuration pages. These pages allow for modification of the system configuration of an installed link. In general, configuration changes can be completed without a reboot. Configuration pages include controls relating to the management agent IP interface, the Ethernet interfaces, quality of service at the wireless interface, security passwords and AES keys.

RADIUS authentication

PTP 800 supports remote authentication for users of the web interface using the Challenge-Handshake Authentication Protocol (CHAP) or Microsoft CHAP version 2 (MS-CHAPv2) over the Remote Authentication Dial-In User Service (RADIUS). PTP 800 supports connections to primary and secondary RADIUS servers. The RADIUS interface is configured through the RADIUS Authentication page of the web-based interfaces.

PTP 800 RADIUS supports the standard Service Type attribute to indicate authentication roles of System Administrator and Read Only together with a vendor specific attribute to indicate authentication roles of Security Officer, System Administrator, and Read Only.

Remote authentication can be used in addition to local authentication, or can be used as a replacement for local authentication. If remote and local authentications are used together, PTP 800 checks log in attempts against locally stored user credentials before submitting a challenge and response for remote authentication. Remote authentication is not attempted if the username and password match locally stored credentials.

RADIUS is only available when PTP 800 is configured for Identity-based User Accounts. For more information, refer to Planning for RADIUS operation on page 2-28.

Email alerts

The management agent can be configured to generate alerts by electronic mail when any of the following events occur:

- Wireless link up
- Wireless link down
- Data port up
- Data port down
- Management port up
- Management port down
- Link name mismatch
- Alignment mode
- Unit out of calibration
- Encryption enabled mismatch
- Data port disabled warning
- Data port fiber status
- Data port configuration mismatch
- SNTP sync
- Management port disabled warning
- RFU status
- Management port configuration mismatch
- Wireless link status
- Protection interface status

Email alerts are described in Managing alarms and events on page 7-15.

SNMP

The management agent supports fault and performance management by means of an SNMP interface. The management agent is compatible with SNMP v1 and SNMP v2c, using the following MIBs:

- PTP 800 enterprise MIB
- The system group and the interfaces group from MIB-II, RFC-1213
- The interfaces group and the ifXTable from RFC-2233
- The dot1dBase group and the dot1dBasePortTable group from the Bridge MIB, RFC-1493.

The PTP 800 enterprise MIB is available for download in the application software package from the support web page (see Contacting Cambium Networks on page 2).

Further details of the standard SNMP MIB objects supported by PTP 800 are provided in Standard SNMP MIBs on page 4-77.

SNMP must be enabled for use by means of the SNMP State attribute in the web-based interface. Activation of SNMP in PTP 800 requires a reboot of the CMU.

The web-based interface must be used to configure the destination IP address for SNMP notifications, and to enable or disable generation of each supported SNMP notification. Supported notifications are as follows:

- Cold start
- Link up
- Link down
- Link name mismatch
- Alignment mode
- Unit out of calibration
- Encryption enabled mismatch
- Data port disabled warning
- Data port fiber status
- Data port configuration mismatch
- SNTP sync
- Management port disabled warning
- RFU status
- Management port configuration mismatch
- Wireless link status
- Protection interface status
- Wireless receive status
- Licensed transmit capacity
- Wireless receive mismatch
- Data port Ethernet speed mismatch
- Management port Ethernet speed mismatch

SNMP notifications are described in Managing alarms and events on page 7-15.

Simple Network Time Protocol (SNTP)

The clock supplies accurate date and time information to the system. It can be set to run with or without a connection to one or two network time servers (SNTP). It can be configured to display local time by setting the time zone and daylight saving in the Time Configuration web page.

If an SNTP server connection is available, the clock can be set to synchronize with the server time at regular intervals. For secure applications, the PTP 800 can be configured to authenticate received NTP messages using the DES or MD5 protocol.

SNMPv3 security

SNMP Engine ID

PTP 800 supports three different formats for SNMP Engine ID:

- MAC address
- IP address
- Configurable text string

SNMPv3 security configuration is re-initialized when the SNMP Engine ID is changed.

User-based security model

PTP 800 supports the SNMPv3 user-based security model (USM) for up to 10 users, with MD5, SHA-1, DES and (subject to the license key) AES protocols in the following combinations:

- No authentication, no privacy,
- MD5, no privacy,
- SHA-1, no privacy,
- MD5, DES,
- SHA-1, DES,
- MD5, AES,
- SHA-1, AES.

Use of AES privacy requires the AES upgrade described in AES license on page 1-60. The system will allow the creation of users configured with AES privacy protocol, regardless of license key. However, a user configured to use AES privacy protocol will not be able to transmit and receive encrypted messages unless the license key enables the AES capability.

View-based access control model

PTP 800 supports the SNMPv3 view-based access control model (VACM) with a single context. The context name is the empty string. The context table is read-only, and cannot be modified by users.

Access to critical security parameters

The SNMPv3 management interface does not provide access to critical security parameters (CSPs). It is not possible to read or modify AES keys used to encrypt data transmitted at the wireless interface.

MIB-based management of SNMPv3 security

PTP 800 supports a standards-based approach to configuring SNMPv3 users and views through the SNMP MIB. This approach provides maximum flexibility in terms of defining views and security levels appropriate for different types of user.

The system provides a default SNMPv3 configuration. This initial configuration is not secure, but it provides the means by which a secure configuration can be created using SNMPv3.

The secure configuration should be configured in a controlled environment to prevent disclosure of the initial security keys necessarily sent as plaintext, or sent as encrypted data using a predictable key. The initial security information should not be configured over an insecure network.

The default configuration is restored when any of the following occurs:

- All CMU configuration data is erased.
- All SNMP users are deleted using the SNMP management interface.
- The SNMP Engine ID Format has been changed.
- The SNMP Engine ID Format is IP Address AND the IP Address has been changed.
- The SNMP Engine ID Format is Text String AND the text string has been changed.
- The SNMP Engine ID Format is MAC Address AND configuration has been restored using a file saved from a different unit.
- SNMPv3 Security Management is changed from web-based to MIB-based.

The default user configuration is specified in SNMPv3 default configuration (MIB-based) on page 2-27.

The system creates the `initial` user and template users with localized authentication and privacy keys derived from the passphrase string `123456789`. Authentication keys for the templates users are fixed and cannot be changed. Any or all of the template users can be deleted.

The default user `initial` is created with a view of the entire MIB, requiring authentication for SET operations. There is no access for template users.

> **NOTE**
> VACM grants access for requests sent with more than the configured security level.

The default user `initial` will have read/write access to the whole of the MIB. This is described in further detail in View-based access control model on page 1-57. The template users have no access to the MIB in the default configuration. User initial will normally be used to create one or more additional users with secret authentication and privacy keys, and with appropriate access to the whole of the MIB or to particular views of the MIB according to the operator's security policy. New users must be created by cloning template users. The user initial may then be deleted to prevent access using the well-known user name and keys. Alternatively, the keys associated with initial may be set to some new secret value.

Web-based management of SNMPv3 security

PTP 800 supports an alternative, web-based approach for configuring SNMPv3 security. In this case, the web-based interface allows users to specify SNMPv3 users, security levels, privacy and authentication protocols, and passphrases. Web-based management will be effective for many network applications, but the capabilities supported are somewhat less flexible than those supported using the MIB-based security management.

Selection of web-based management for SNMPv3 security disables the MIB-based security management.

Web-based management of SNMPv3 security allows for two security roles:

- Read Only
- System Administrator

Read Only and System Administrator users are associated with fixed views allowing access to the whole of the MIB, excluding the objects associated with SNMPv3 security. System Administrators have read/write access as defined in the standard and proprietary MIBs.

Web-based management of SNMPv3 security allows an operator to define the security levels and protocols for each of the security roles; all users with the same role share a common selection of security level and protocols.

Web-based security configuration is re-initialized when any of the following occurs:

- All CMU configuration data is erased.
- The SNMP Engine ID Format has been changed.
- The SNMP Engine ID Format is IP Address and the IP Address has been changed.
- The SNMP Engine ID Format is Text String and the text string has been changed.
- The SNMP Engine ID Format is MAC Address and configuration has been restored using a file saved from a different unit.

- SNMPv3 Security Management is changed from MIB-based to web-based.

Additionally, all SNMP user accounts are disabled when the authentication protocol, the privacy protocol, or the security level is changed.

Downgrade of the license key

A possible lockout condition exists if a user downgrades the license key so as to disable the AES capability when SNMPv3 users are configured with AES privacy and VACM is configured to require privacy. In this case, recovery is by either (a) restoring the correct license key, or (b) using recovery mode to erase all configuration and entering new configuration.

Option (b) will cause default users and access configuration to be re-created.

System logging (syslog)

PTP 800 supports the standard syslog protocol to log important configuration changes, status changes and events. The protocol complies with RFC 3164.

PTP 800 creates syslog messages for configuration changes to any attribute that is accessible via the web-based interface, or via the enterprise MIB at the SNMP interface.

PTP 800 additionally creates syslog messages for changes in any status variable displayed in the web-based interface.

PTP 800 creates syslog messages on a number of events (for example successful and unsuccessful attempts to log in to the web-based interface).

PTP 800 can be configured to send syslog messages to one or two standard syslog servers.

Additionally, PTP 800 logs event notification messages locally. Locally-stored event messages survive reboot of the unit, and are overwritten only when the storage capacity is exhausted (approximately 2000 messages). The locally stored events can be reviewed using the web-based user interface.

Only users with ‘Security Officer’ role are permitted to configure the syslog client. Users with Security Officer, System Administrator or Read Only roles are permitted to review the locally logged event messages.

AES license

PTP 800 provides optional encryption using the Advanced Encryption Standard (AES). Encryption is not available in the standard system.

AES upgrades are supplied as an access key purchased from your Cambium Point-to-Point distributor or solutions provider. The access key authorizes AES operation for one CMU. Two access keys are needed to operate AES on a link. The upgrade is applied by entering an access key together with the MAC address of the target CMU into the PTP License Key Generator web page, which may be accessed from the support web page (see Contacting Cambium Networks on page 2).

The License Key Generator creates a new license key that is delivered by email. The license key must be installed on the CMU. When the license key is installed, the CMU must be rebooted before AES can be enabled. Once applied, the AES upgrade is bound to a single CMU and is not transferrable.

AES encryption may be used in the following ways:

- At the wireless port to encrypt data transmitted over the wireless link.
- At the SNMP management interface in the SNMPv3 mode.
- At the HTTPS/TLS management interface.

Two levels of encryption are available to purchase:

- 128-bit: This allows an operator to encrypt all traffic sent over the wireless link using 128-bit encryption.
- 256-bit: This allows an operator to encrypt traffic using either 128-bit or 256-bit encryption.

Encryption must be configured with the same size key in each direction.

AES encryption at the wireless port is based on pre-shared keys. An identical key must be entered at each end of the link.

AES encryption for SNMPv3 is always based on a 128-bit key, regardless of level enabled in the license key.

For more information, see:

- Task 3: Installing license keys on page 6-21
- Task 5: Configuring security on page 6-28

Login information

PTP 800 optionally provides details of the most recent successful login, and the most recent unsuccessful login attempt, for each user of the web-based interface.

Flexible capacity upgrades

The maximum data throughput capacity of the PTP 800 wireless link is the lower of the wireless link capacity and the data capacity limit set by the PTP 800 license key.

All PTP 800 CMUs are shipped with a factory-set 10 Mbps capacity limit, meaning that capacity is restricted to a maximum of 10 Mbps at the data port. Users can purchase capacity upgrades in nine steps between 20 Mbps and unlimited capacity. Upgrades are applied through the CMU license key, without any change to the hardware. Capacity may be different for different directions.

NOTE

Full capacity trial period: New PTP 800 units can be configured to operate with full transmit capacity (unlimited) during a trial period of duration 60 days, reverting to the licensed capacity when the trial period expires. This trial period is also available on existing units that are upgraded to System Relelease 800-04-00 (or later) from an earlier release.

Capacity upgrades are supplied as an access key. The access key authorizes a specific capacity limit for one CMU. Two access keys are needed to operate a link at enhanced capacity. The upgrade is applied by entering an access key together with the MAC address of the target CMU into the PTP License Key Generator web page, which may be accessed from the support web page (see Contacting Cambium Networks on page 2).

This web page generates a new license key that must be installed on the CMU. Capacity upgrades become active as soon as the license key is validated. There is no need to reboot the CMU, and the upgrade process does not involve a service interruption. Once applied, the capacity upgrade is bound to a single CMU and is not transferrable.

For ordering details including Cambium part numbers, refer to Ordering capacity upgrades on page 2-97.

Software upgrade

The management agent supports application software upgrade using the web-based interface.

PTP 800 software images are digitally signed, and the CMU will accept only images that contain a valid Cambium PTP digital signature. The CMU always requires a reboot to complete a software upgrade.

The CMU application software image contains an embedded software image for the RFU. If a CMU software upgrade introduces a new RFU software version, then the RFU software is upgraded automatically following reboot of the CMU.

> **NOTE**
>
> Obtain the application software and this user guide from the support website BEFORE warranty expires.
>
> CMU software version must be the same at both ends of the link. Limited operation may sometimes be possible with dissimilar software version, but such operation is not supported by Cambium.

The management process for software upgrade is described in detail in Task 4: Upgrading software version on page 6-25.

Software can be downgraded using Recovery mode as described in Downgrading PTP 800 software on page 7-77.

Recovery mode

The PTP 800 recovery mode provides a means to recover from serious configuration errors including lost or forgotten passwords and unknown IP addresses.

Recovery mode also allows new main application software to be loaded even when the integrity of the existing main application software image has been compromised. The most likely cause of an integrity problem with the installed main application software is where the power supply has been interrupted during an earlier software upgrade.

The CMU operates in recovery mode in the following circumstances:

- When a checksum error occurs for the main application software image.
- When the CMU front panel recovery button is pressed at the same time as the CMU is rebooted or power cycled.
- When the Short Power Cycle for Recovery is enabled, and CMU is power cycled, and the “off” period is between one and five seconds.

Options in recovery mode are as follows:

- Load new main application software.
- Reset all configuration data to factory default. This option resets IP and Ethernet configuration, and erases (zeroizes) critical security parameters.
- Reset IP and Ethernet configuration to factory default.
- Erase (zeroize) critical security parameters.
- Reboot with existing software and configuration.

NOTE

If recovery mode has been entered either because of a checksum error or Short Power Cycle, by default the CMU will reboot with existing software and configuration following a 30 second wait.

The recovery software image is installed during manufacture of the CMU and cannot be upgraded by operators.

For detailed instructions on using the recovery mode, see Using recovery mode on page 7-71.

Further reading on system management

For more information on system management, refer to the following:

- Security planning on page 2-22 describes how to plan for PTP 800 links to operate in secure modes, including HTTPS/TLS, SNMP and SNMPv3.
- Chapter 6: Configuration and alignment describes all configuration and alignment tasks that are performed when a PTP 800 link is deployed.
- Chapter 7: Operation provides instructions for operators of the PTP 800 web user interface.

1+1 Hot Standby link protection

This section is an overview of the concept, operation and interfaces of 1+1 Hot Standby links.

1+1 Hot Standby overview

The 1+1 Hot Standby feature provides an option for protecting against a single point equipment failure. It also enables maintenance to be carried out with insignificant impact on customer traffic. Such maintenance actions include software upgrade and unit replacement.

In order to protect against failure, extra equipment is required to be installed at each end of the link compared to a standard 1+0 link. This extra equipment will remain on standby until it is required to take over in case of equipment failure.

Each end of a 1+1 Hot Standby consists of two CMUs, and either two ODUs for outdoor deployments or one 1+1 capable IRFU for indoor deployments. The 1+1 capable IRFU contains two transceivers for the purposes of protection. In addition, each end can be deployed with either one or two antennas depending on the customer requirements. The antenna options are described in 1+1 Hot Standby link antenna options on page 1-65. At the network side, at least one Ethernet switch must be installed at each end of the link. Detailed network options are described in Planning 1+1 Hot Standby links on page 2-35.

The two CMUs which are installed at the same end of a 1+1 Hot Standby link exchange information over an interface known as the Protection Interface. This shares the same physical socket as the Management Port. For configurations which manage the CMU over the Management Port, an accessory known as the Out of Band Protection Splitter is required. This splits out the management traffic from the protection interface.

The 1 + 1 Hot Standby feature is only supported in CMUs with Boot Monitor software Boot-03-00 or later.

Active and inactive units

At any one time at a given end of a 1+1 Hot Standby link, only one CMU will provide the function of forwarding Ethernet frames between the wireless interface and the Ethernet interface. Also, only the ODU / IRFU transceiver connected to this CMU will radiate at the antenna. These units are called the active units.

The other CMU and ODU / IRFU transceiver are called the inactive units and these will remain on standby waiting to take over in case of a failure of the active units. If a failure does occur, an automatic protection switch will take place and the previously inactive units will take over as the active units. A protection switch may take place at one end of the link independently of the other end of the link. A protection switch may also be executed by management action.

Primary and secondary units

At each end of the link, one CMU must be configured as a Primary unit, the other as a Secondary unit. The decision of whether the Primary or Secondary CMU becomes active is automatically controlled by the CMU application software. In normal fault free conditions, the CMU application software will select the Primary CMU and associated ODU / IRFU transceiver to be the active unit.

1+1 Hot Standby link antenna options

Single antenna per end

The ODUs installed at the same end of a 1+1 Hot Standby link can share an antenna. This is done with an ODU Coupler Mounting Kit (Figure 23). The Coupler Mounting Kit can be supplied with equal or unequal coupling. The equal coupler provides the same path loss to the two ODUs where as the unequal coupler provides a lower path loss to one of the ODUs. As the unit configured as Primary is expected to be the active unit for most of the life of a 1+1 Hot Standby link, the highest link availability is achieved by connecting the Primary ODU to the arm of the unequal coupler with the lowest path loss.

IRFUs with the 1+1 Tx MHSB option are designed to connect to a single antenna via elliptical waveguide. Although this IRFU option is supplied with two transceivers, only the active transceiver will radiate at the antenna port. This is achieved by an RF switch which is an integral part of the 1+1 IRFUs. The position of the switch is controlled by the CMU application software. The RF switch is not used for the receive direction and both transceivers will simultaneously receive from this same antenna. This is achieved through the use of a coupler which is internal to the IRFU. The 1+1 Tx MHSB option can be supplied with equal or unequal receiver coupling. For more information on the IRFU options, please refer to Planning 1+1 Hot Standby links on page 2-35.

Two antennas per end

The ODUs installed at the same end of a 1+1 Hot Standby link can be connected to separate antennas. Although antennas with different gains or mounting options may be deployed, they must have the same polarization. If the two antennas at a given end have different gains, the ODU configured as Primary should be connected to the antenna with the highest gain. This option is generally used to provide Spatial Diversity however it also provides protection in the case of antenna or waveguide failure.

IRFUs with the 1+1 Tx MHSB / RX SD option are designed to connect to two antennas via elliptical waveguide, a main antenna and a diverse antenna. However the IRFU will only ever radiate from the main antenna, the transceivers being routed to this antenna by an RF switch in an identical way to the 1+1 Tx MHSB option. In the receive direction, Spatial Diversity is achieved by the main antenna connecting to one transceiver and the diverse antenna connecting to the other transceiver. Although antennas with different gains may be deployed, they must have the same polarization. For more information about Spatial Diversity, refer to Receive Diversity on page 1-67.

Bridging in 1+1 links

Only the active CMU forwards customer data from the wireless interface to the Ethernet switch. Also, when Out of Band Management is enabled, only the active CMU forwards management data received from the wireless interface to the Ethernet Switch.

In the reverse direction only the active CMU forwards customer and management frames to the wireless interface. This includes management frames which are sourced by the CMU. When a protection switch occurs, the Ethernet Switch learns to send traffic to the newly active CMU. This is achieved by the newly Inactive CMU momentarily disabling its Ethernet ports which causes the Ethernet Switch to flush its forwarding data base and learn the new path.

> **NOTE**
> The selected Ethernet Switch must support the feature of flushing the forwarding data base on port down.

The Inactive CMU is only manageable from its local Ethernet Port. This is the Data Port when configured for In Band operation and the Management Port when configured for Out of Band operation. Remote management of the Inactive CMU is still possible across the wireless link, the active CMU forwarding management traffic received on the wireless interface to Ethernet Switch which in turn forwards on to the Inactive CMU.

Receive Diversity

Receive Diversity improves link availability by providing each end of a wireless link with multiple observations of the signal which has been transmitted from the remote end of the link. It is particularly effective in combating multipath fading caused by atmospheric effects such as scintillation and ducting. Both these effects can occur to a significant degree in microwave links. It also combats fading caused by reflections from water.

Receive Diversity can be enabled (at the CMU) in any of the supported 1+1 Hot Standby configurations. When Receive Diversity is enabled, the Active CMU examines the quality of the data which has been received from the wireless interface of both neighbour CMUs and selects the best data on a byte by byte basis.

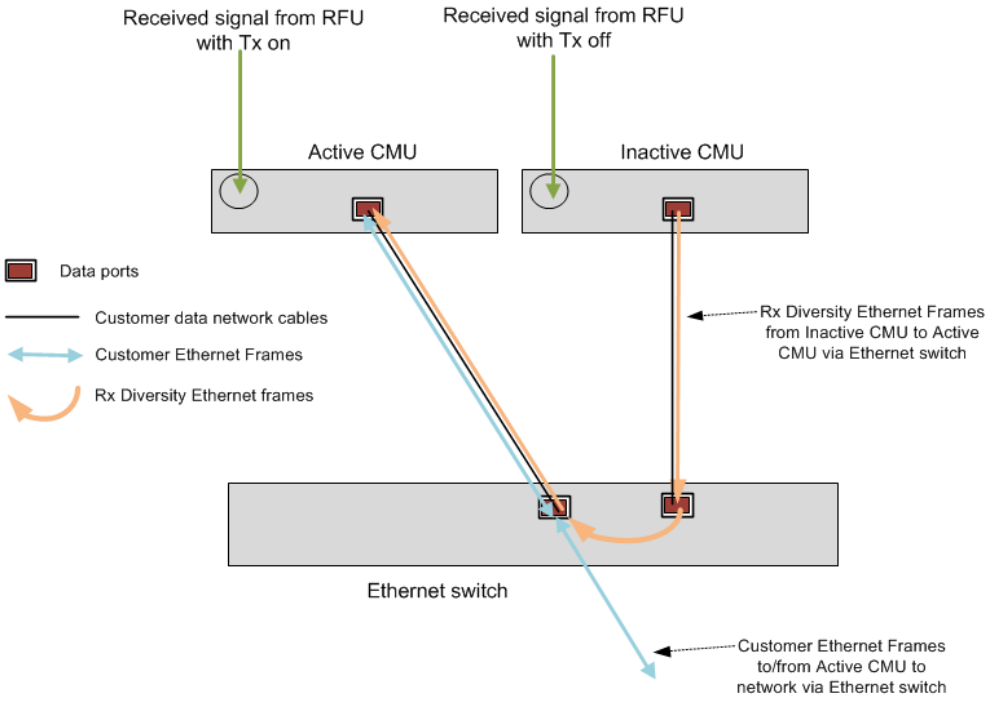
NOTE

If separate antennas are installed at each end, then Receive Spatial Diversity is achieved.

Receive Diversity Ethernet frames

An important aspect of Receive Diversity is how the data received at the wireless interface of the Inactive CMU arrives at the Active CMU. This is achieved by the Inactive CMU encapsulating the received wireless data into Ethernet frames and sending the frames out on the Data port at a constant rate. This requires that the Data ports and also the ports to which they connect at the Ethernet switch are configured into a VLAN dedicated to Receive Diversity Ethernet frames (Figure 35).

Figure 35 Receive Diversity Ethernet frames


Received signal from RFU with Tx on
Received signal from RFU with Tx off
Active CMU
Inactive CMU
Data ports
Customer data network cables
Customer Ethernet Frames
Rx Diversity Ethernet frames
Rx Diversity Ethernet Frames from Inactive CMU to Active CMU via Ethernet switch
Ethernet switch
Customer Ethernet Frames to/from Active CMU to network via Ethernet switch

Effects of Receive Diversity on 1+1 operation

In almost all aspects, the 1+1 Hot Standby feature operates in the same way regardless of whether or not Receive Diversity has been enabled. Of most significance is the concept of the Active and Inactive units, where it is the Active ODU or IRFU transceiver which always radiates at the antenna and the Active CMU which forwards Ethernet frames to the network. The Inactive unit remains on standby to take over the role of the Active unit in case of a fault. However, there are some subtle differences as follows:

- When Receive Diversity is enabled, then a protection switch will not occur if the fault only affects the wireless receiver of the Active CMU, ODU or IRFU transceiver. This is because the Active CMU will seamlessly use the data received at the wireless interface of the Inactive CMU. The Active ODU or IRFU transceiver will continue to radiate at the antenna. Receiver faults in this category are the RFU Rx Synthesizer faults and complete loss of the wireless receive signal.
- The Fiber-Y configuration is useful in a network which requires a single Ethernet interface for customer traffic. In order to support Receiver Diversity in Fiber-Y configurations, the CMU copper data ports must also be connected to the same Ethernet Switch as the Fiber-Y interface. This is because the Fiber port of the Inactive CMU is necessarily disabled in Fiber-Y configurations. The copper port is therefore required in order for the Inactive CMU to send Receive Diversity Ethernet Frames. Note that the copper port will never carry customer traffic hence the single interface for customer traffic is not compromised.

NOTE

When Receive Diversity is enabled, there is a small impact on maximum Latency, and hence jitter. When there is significant fading and the Active CMU is using data which has been received at the wireless interface of the Inactive CMU, the latency increase will be affected by the customer traffic. The worst case is where jumbo frames are included in the customer traffic in which case the maximum increase in latency will be 150 μs. In periods where there is no significant fading, the Active CMU will use the data from its own wireless receiver in which case there will be a fixed increase in maximum latency of 12 μs.

Further reading on 1+1 Hot Standby

For more information on 1+1 Hot Standby link protection, refer to the following:

- Planning 1+1 Hot Standby links on page 2-35 describes factors to be considered when planning a 1+1 Hot Standby link.
- Protection interface specifications on page 4-17 contains specifications of components used in 1+1 protection interfaces.
- Upgrading an unprotected link to on page 6-61 describes how to upgrade an existing unprotected link to use the 1+1 Hot Standby link protection feature.
- Installing antennas and ODUs on page 5-5 describes how to connect one antenna to two ODUs via a coupler, either in a direct mount or remote mount configuration.
- Preparing network connections (1+1 Hot Standby) on page 5-89 describes how to connect the CMUs to the network equipment for 1+1 Hot Standby links.
- Upgrading software in an operational 1+1 Hot Standby link on page 7-69 describes how to manage software upgrades in 1+1 Hot Standby links.
- Task 6: Configuring protection on page 6-53 describes how to configure the CMUs as two pairs of protected units.
- Aligning protected antennas on page 6-99 describes the alignment process for a 1+1 Hot Standby link with two antennas at each end.
- Managing 1+1 Hot Standby links on page 7-33 describes how to use the Protected Link web page.
- Testing protection switchover on page 8-13 describes the tests to be performed if any problems are experienced with protection switchovers in a newly installed (or operational) 1+1 Hot Standby link.

FIPS 140-2

This section describes the (optional) FIPS 140-2 cryptographic mode of operation.

PTP 800 provides an optional secure cryptographic mode of operation validated to Level 1 of Federal Information Processing Standards Publication 140-2.

FIPS 140-2 capability

A PTP 800 unit is capable of operating in the FIPS 140-2 mode when all of the following are true:

- The CMU license key has AES encryption enabled.
- The CMU license key has FIPS operation enabled.
- The CMU software image is validated for FIPS operation.
- The CMU tamper evident label has not be interfered with (Figure 36).

Figure 36 Tamper evident label on rear edge of CMU



Validated software image

FIPS validated software images are indicated by a `-FIPS` suffix to the file name, for example: `PTP800-04-10-FIPS.DLD2`. The general features of a FIPS validated software image are identical to those of the standard image with the same version number. For example, `PTP800-04-10-FIPS.DLD2` is equivalent to `PTP800-04-10.DLD2` apart from the ability of the FIPS image to operate in FIPS mode.

Indication of FIPS 140-2 capability

The FIPS 140-2 capability is indicated by a distinctive symbol displayed at the top of the navigation bar in the web-based interface, as shown in Figure 37.

Figure 37 Indication of FIPS 140-2 capability



FIPS 140-2 mode

PTP 800 operates in the FIPS 140-2 mode when all of the following are true:

- The PTP 800 is FIPS 140-2 capable.
- The HTTPS/TLS management interface is enabled.
- The HTTP management interface is disabled.
- The Telnet management interface is disabled.
- SNMP control of HTTP and Telnet is disabled.
- AES encryption is enabled at the wireless interface.
- The HTTPS/TLS management interface is configured for identity-based user accounts.
- RADIUS authentication of web-based users is disabled.

FIPS operational mode alarm

The FIPS operational mode alarm indicates that the unit is FIPS 140-2 capable, but has not been configured correctly for FIPS 140-2 operation. The FIPS operational mode alarm appears as shown in Figure 38.

Figure 38 FIPS operational mode alarm

System Summary

Attributes	Value	Units
Wireless Link Status	Searching	
Link Name	FIPS 140-2 test	
Elapsed Time Indicator	19:30:53	
System Clock	16-Apr-2010 08:01:00	
Fips Operational Mode Alarm	FIPS mode is not configured	

Indication of FIPS 140-2 mode

The PTP 800 is operating in FIPS 140-2 mode when the FIPS 140-2 capability logo is displayed in the navigation bar and the FIPS Operational Mode Alarm is absent from the Home page.

Exiting from the FIPS 140-2 operational mode

A PTP 800 in FIPS 140-2 operational mode can be prepared to accept new security configuration by zeroizing critical security parameters (CSPs). The unit remains FIPS 140-2 capable.

Reverting to standard operation

A FIPS 140-2 capable CMU can be used in standard (non-FIPS) mode by loading a standard (non-FIPS) software image and rebooting.

The critical security parameters (CSPs) are zeroized when the unit is no longer FIPS 140-2 Capable.

Further reading on FIPS 140-2

For more information on FIPS 140-2, refer to the following:

- Planning for FIPS 140-2 operation on page 2-24 describes how to prepare for FIPS 140-2 operation by obtaining the required cryptographic material and by configuring the PTP 800 system.
- Configuring for FIPS 140-2 applications on page 6-121 is a summary of all the configuration tasks that are necessary if the unit is to operate in FIPS 140-2 secure mode.
- Task 3: Installing license keys on page 6-21 describes how to ensure that FIPS 140-2 operation is enabled by license key.
- Task 4: Upgrading software version on page 6-25 describes how to ensure that the installed software version is FIPS 140-2 validated.
- Task 5: Configuring security on page 6-28 describes how to to configure the PTP 800 in accordance with the network operator’s security policy.
- Exiting FIPS 140-2 mode on page 7-51 describes how to disable FIPS 140-2 operation.

Chapter 2: Planning considerations

This chapter describes how to plan a PTP 800 link.

The following topics are described in this chapter:

- Link planning on page 2-2 describes factors to be taken into account when planning PTP 800 links, such as site selection and cable length, and it introduces the PTP LINKPlanner.
- Grounding and lightning protection on page 2-7 describes the grounding and lightning protection requirements of PTP 800 installations.
- Data network planning on page 2-18 describes factors to be considered when planning PTP 800 data networks.
- Security planning on page 2-22 describes how to plan for PTP 800 links to operate in secure mode.
- Planning 1+1 Hot Standby links on page 2-35 describes how to plan a 1+1 Hot Standby link to provide Hot Standby link protection.
- Ordering components on page 2-57 describes how to select components for a planned PTP 800 link (as an alternative to PTP LINKPlanner). It specifies Cambium part numbers for PTP 800 components.

Link planning

When planning the link, follow the high level process described in this section. Take account of factors such as site selection, wind loading, cable length and power supply. Use PTP LINKPlanner as a tool to plan the link.

Process

The majority of the 6 to 38 GHz spectrum is licensed on a link by link basis. Adapt the planning process to suit the licensing regime that is in force in the country of operation.

To plan the link, follow this high-level process:

1. Identify suitable sites at the ends of the link.
2. Determine the data capacity and availability required for the link.
3. Select an RF band, taking into account the range of link, the capacity required, the availability required, the licensing policy for bands in the region or country, and likely availability of individual licenses in that band.
4. Decide whether or not Spatial Diversity is required. Regulations may mandate, or at least recommend Spatial Diversity for certain lengths of link. Use PTP LINKPlanner to estimate the performance increase provided by enabling Spatial Diversity.
5. Decide whether or not to deploy 1+1 Hot Standby. This may be required for very critical links where outages due to equipment failure cannot be tolerated. If Spatial Diversity is selected, 1+1 Hot Standby automatically becomes available.
6. Decide whether to install the Radio Frequency Units on the mast (ODU) or indoors (IRFU). Use the same option at both ends of the link.
7. Use PTP LINKPlanner to check that a satisfactory, unobstructed, line-of-sight path is possible between the ends.
8. Use PTP LINKPlanner to estimate the performance increase provided by enabling ACM.
9. Apply for an individual license.
10. Use PTP LINKPlanner with the license details to identify a Bill of Materials for the link.
11. Order equipment from Cambium.

Cambium offers a license coordination service for links in the USA. The service includes link study, PCN, FCC application filling, Schedule-K completion and one year license protection warranty. To order the FCC Microwave license coordination service from Cambium, quote part number WB3659.

Site selection

To provide a clear line-of-sight path for the link, mount the antennas where they are elevated above their immediate surroundings and above obstructions. Use LINKPLanner to determine suitable antenna heights to clear the terrain. Conduct a site survey to ensure that there are no other obstacles.

Wind loading

Select a site where the wind load will not be too high. For all the antennas supplied by Cambium, the maximum permitted wind velocities are:

- Operational wind velocity: 113 km/h (70 mph)
- Peak survival wind velocity: 249 km/h (155 mph)

Maximum IF cable length

> **NOTE**
> Applies to ODU deployments only.

Select a site where the IF cable will not be too long. The maximum permitted IF cable lengths are:

- 190 meters (620 ft) with CNT-400 or equivalent cable.
- 300 meters (970 ft) with CNT-600 or equivalent cable.

Power supply considerations

Confirm that the planned site has a power supply that meets the following requirements:

- It is possible to remove power from the CMU and IRFU (if installed) without disrupting other equipment, for example a circuit breaker.
- If the link is protected, it is possible to remove power from one PTP 800 without disrupting the other PTP 800.
- Circuit breakers and switches are clearly labeled.
- Wiring from the power source to the PTP 800 is sized accordingly.
- All supply wiring conforms to national standards and best practice.
- A rack mounted power supply is grounded in accordance with national standards and best practice.

For more information, refer to AC to DC converter specifications on page 4-4.

⚠ CAUTION

Provide a 4 Amp fuse or similar protection device between the –48 V dc supply source and the PTP 800 CMU and IRFU (if installed).

Always ensure that the power supply is turned off before attempting any service on the PTP 800 installation.

The CMU and IRFU (if installed) are positive ground and the DC power supply or battery must also be positive ground or isolated.

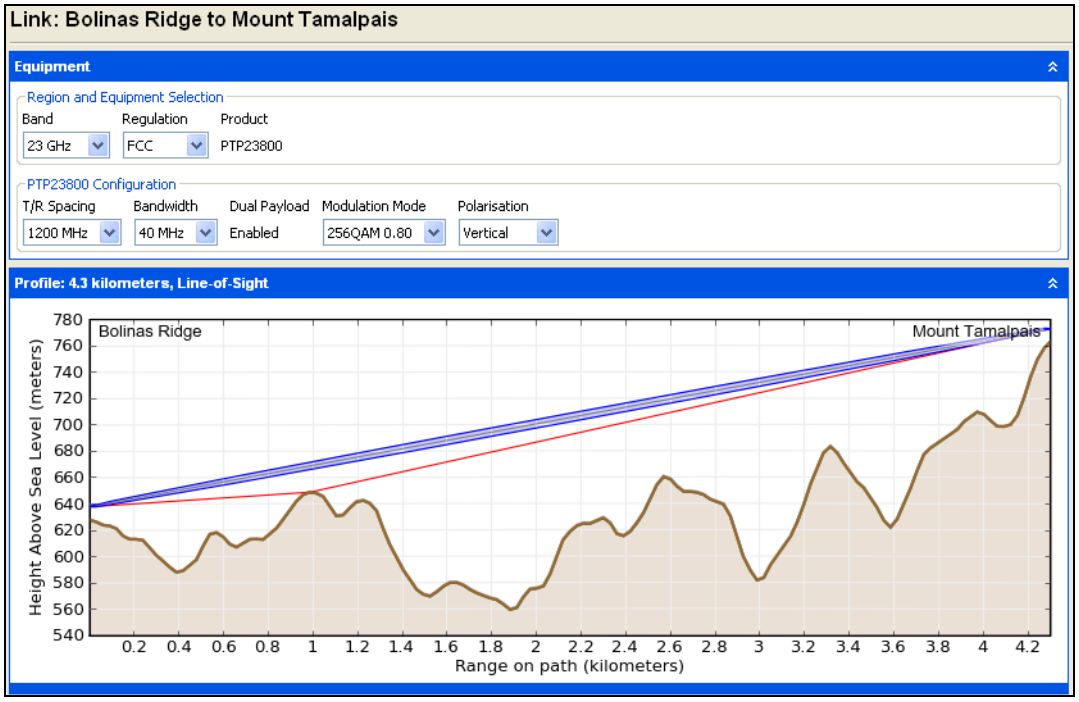
PTP LINKPlanner

Use the Cambium PTP LINKPlanner to design PTP 800 links. This is a link planning and optimization tool designed for use with all PTP products. PTP LINKPlanner is free and available from the support web page (see Contacting Cambium Networks on page 2). The advantages of PTP LINKPlanner are as follows:

- It is supported on Windows and Macintosh Platforms.
- It is very easy to use without specialist radio planning knowledge.
- It is powerful, implementing the latest ITU recommendations for predicting the performance of a radio link.
- It expresses the performance in terms of data link capacity.
- It is integrated with Google Earth™ to facilitate site entry and path visualization.
- It provides bill of materials data for ease of purchasing.
- It can provide path data by an automated email service.
- It can model all Cambium PTP products.
- It can plan multiple links in the same session.
- It can generate an export file for Cambium's FCC Coordination service.

The PTP LINKPlanner provides path profile information for individual links as shown in Figure 39.

Figure 39 LINKPlanner profile view



The PTP LINKPlanner also provides configuration and performance details as shown in Figure 40, and Bill of Materials data as shown in Figure 41.

This is necessarily a brief introduction to the PTP LINKPlanner. Please download and evaluate this free software in further detail.

Figure 40 LINKPlanner configuration and performance details

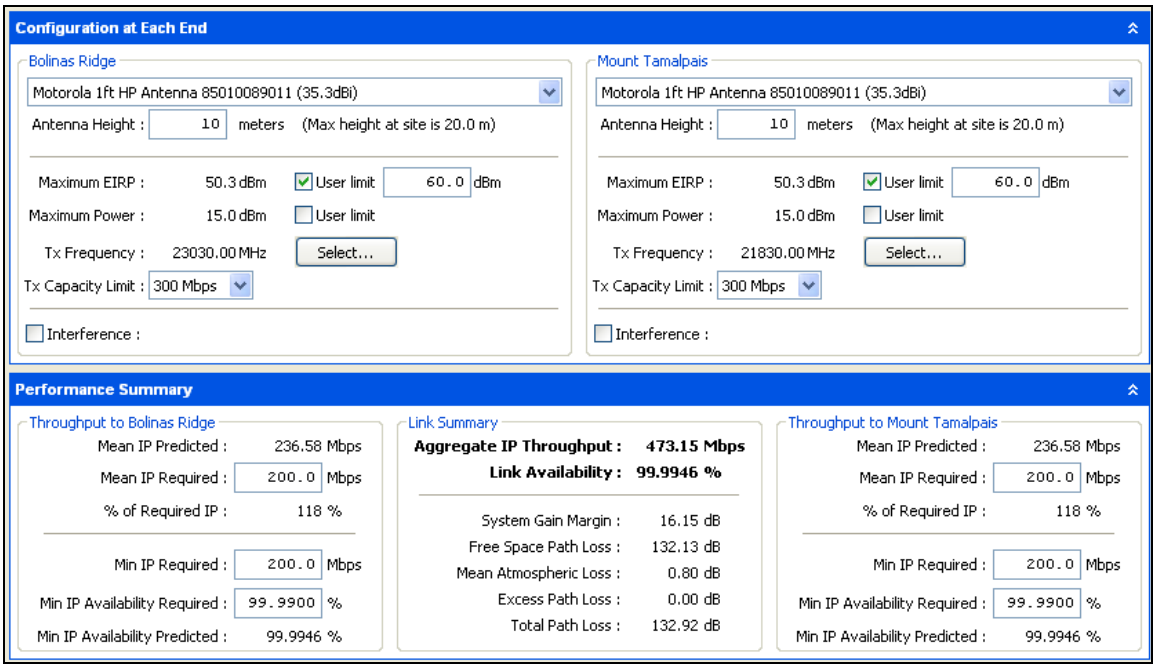
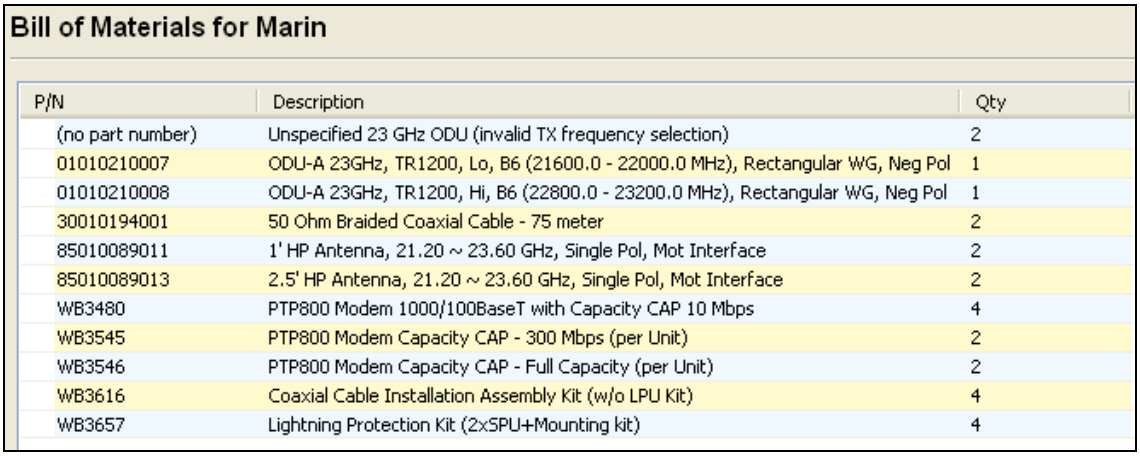

Configuration at Each End
Bolinas Ridge
Motorola 1ft HP Antenna 85010089011 (35.3dBi)
Antenna Height : 10 meters (Max height at site is 20.0 m)
Maximum EIRP : 50.3 dBm User limit 60.0 dBm
Maximum Power : 15.0 dBm User limit
Tx Frequency : 23030.00 MHz Select...
Tx Capacity Limit : 300 Mbps
Interference :
Mount Tamalpais
Motorola 1ft HP Antenna 85010089011 (35.3dBi)
Antenna Height : 10 meters (Max height at site is 20.0 m)
Maximum EIRP : 50.3 dBm User limit 60.0 dBm
Maximum Power : 15.0 dBm User limit
Tx Frequency : 21830.00 MHz Select...
Tx Capacity Limit : 300 Mbps
Interference :
Performance Summary
Throughput to Bolinas Ridge
Mean IP Predicted : 236.58 Mbps
Mean IP Required : 200.0 Mbps
% of Required IP : 118 %
Min IP Required : 200.0 Mbps
Min IP Availability Required : 99.9900 %
Min IP Availability Predicted : 99.9946 %
Link Summary
Aggregate IP Throughput : 473.15 Mbps
Link Availability : 99.9946 %
System Gain Margin : 16.15 dB
Free Space Path Loss : 132.13 dB
Mean Atmospheric Loss : 0.80 dB
Excess Path Loss : 0.00 dB
Total Path Loss : 132.92 dB
Throughput to Mount Tamalpais
Mean IP Predicted : 236.58 Mbps
Mean IP Required : 200.0 Mbps
% of Required IP : 118 %
Min IP Required : 200.0 Mbps
Min IP Availability Required : 99.9900 %
Min IP Availability Predicted : 99.9946 %

Figure 41 LINKPlanner Bill of Materials view



P/N	Description	Qty
(no part number)	Unspecified 23 GHz ODU (invalid TX frequency selection)	2
01010210007	ODU-A 23GHz, TR1200, Lo, B6 (21600.0 - 22000.0 MHz), Rectangular WG, Neg Pol	1
01010210008	ODU-A 23GHz, TR1200, Hi, B6 (22800.0 - 23200.0 MHz), Rectangular WG, Neg Pol	1
30010194001	50 Ohm Braided Coaxial Cable - 75 meter	2
85010089011	1' HP Antenna, 21.20 ~ 23.60 GHz, Single Pol, Mot Interface	2
85010089013	2.5' HP Antenna, 21.20 ~ 23.60 GHz, Single Pol, Mot Interface	2
WB3480	PTP800 Modem 1000/100BaseT with Capacity CAP 10 Mbps	4
WB3545	PTP800 Modem Capacity CAP - 300 Mbps (per Unit)	2
WB3546	PTP800 Modem Capacity CAP - Full Capacity (per Unit)	2
WB3616	Coaxial Cable Installation Assembly Kit (w/o LPU Kit)	4
WB3657	Lightning Protection Kit (2xSPU+Mounting kit)	4

Grounding and lightning protection

Ensure that the link meets the grounding and lightning protection requirements described in this section.

WARNING

Electro-magnetic discharge (lightning) damage is not covered under warranty. The recommendations in this guide, when followed correctly, give the user the best protection from the harmful effects of EMD. However 100% protection is neither implied nor possible.

The need for power surge protection

Ensure that the planned PTP 800 installation protects structures, equipment and people against power surges (typically caused by lightning) by conducting the surge current to ground via a separate preferential solid path. The actual degree of protection required depends on local conditions and applicable local regulations. Cambium recommends that PTP 800 installation is contracted to a professional installer.

Standards

To gain a full understanding of lightning protection methods and requirements, refer to the international standards IEC 61024-1 and IEC 61312-1, the U.S. National Electric Code ANSI/NFPA No. 70-1984, or section 54 of the Canadian Electric Code.

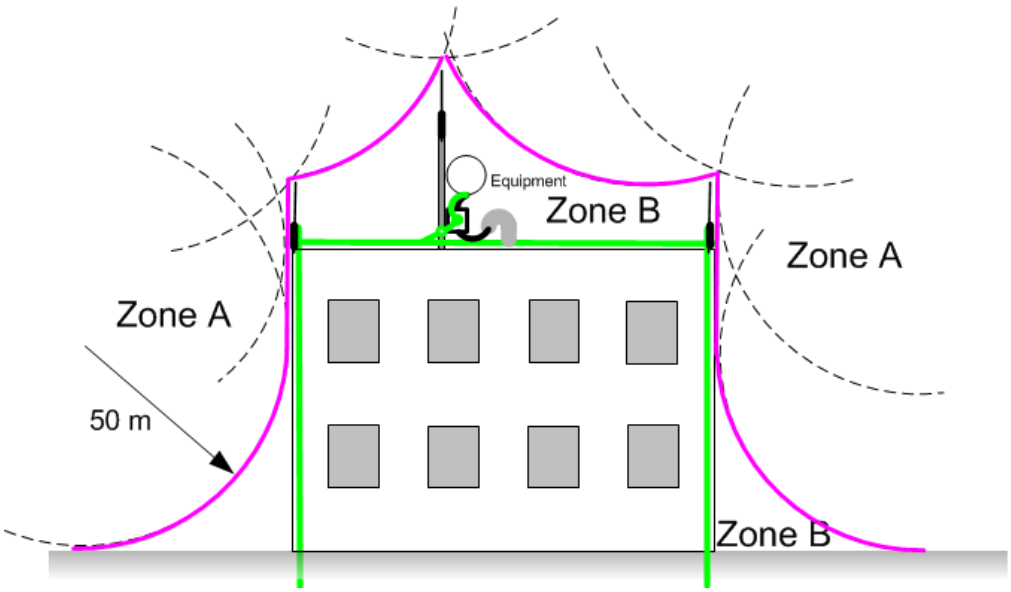
NOTE

International and national standards take precedence over the requirements in this guide.

Lightning protection zones

Use the 'rolling sphere method' (Figure 42) to determine where it is safe to mount equipment. An imaginary sphere, typically 50 meters in radius, is rolled over the structure. Where the sphere rests against the ground and a strike termination device (such as a finial or ground bar), consider the space under the sphere to be in the zone of protection (Zone B). Where the sphere rests on two finials, consider the space under the sphere to be in the zone of protection.

Figure 42 Rolling sphere method to determine the lightning protection zones



Assess locations on masts, towers and buildings to determine if the location is in Zone A or Zone B:

- Zone A: In this zone a direct lightning strike is possible. Do not mount equipment in this zone.
- Zone B: In this zone, direct EMD (lightning) effects are still possible, but mounting in this zone significantly reduces the possibility of a direct strike. Mount equipment in this zone.

⚠ WARNING

Never mount equipment in Zone A. Mounting in Zone A may put equipment, structures and life at risk.

General protection requirements

Ensure that the PTP 800 installation meets the general protection requirements described in this section.

Basic requirements

Install the outdoor equipment, that is antenna and ODU (if deployed), in 'Zone B' (see Lightning protection zones on page 2-8).

Ground the indoor devices, that is CMU and IRFU (if deployed), at their chassis bonding points.

Grounding cable requirements

Use grounding cables that meet the following requirements:

- Grounding cables are no less than 16mm^2 or #6AWG in size, with solid or stranded, tinned and/or jacketed copper conductors.
- Grounding conductor runs are as short, straight, and smoothly as possible, with the fewest possible number of bends and curves.
- Grounding cables are not installed with drip loops.
- All bends have a minimum radius of 203 mm (8 in) and a minimum angle of 90°. A diagonal run is preferable to a bend, even though it does not follow the contour or run parallel to the supporting structure.
- All bends, curves and connections are routed towards the grounding electrode system, ground rod, or ground bar.
- Grounding conductors are securely fastened.
- Braided grounding conductors are not used.
- Approved bonding techniques are employed when connecting dissimilar metals.

LPU and IF cable requirements

> **NOTE**
> Applies to ODU deployments only.

Use LPUs and IF cables that meet the following requirements:

- A lightning protection unit (LPU) (from the Cambium LPU kit, part number WB3657) is installed within 600 mm (24 in) of the point at which the IF cable enters the building or equipment room.
- The IF cable is bonded to the supporting structure in order to prevent lightning creating a potential between the structure and cable, which could cause arcing, resulting in damage to equipment.
- The IF cable is grounded at the building entry point.

Specific requirements for the ODU

> **NOTE**
> Applies to ODU deployments only.

Ensure that all ODU installations meet the following requirements:

- The ODU and top LPU are as close together as possible.
- The IF cable length between the ODU and top LPU is less than 800mm. The cable supplied in the accessory kit meets this requirement.
- The top LPU is mounted lower than the ODU.
- The ODU and top LPU are bonded together with the 800 mm long 16mm^2, #6AWG cable supplied in the accessory kit.
- The LPU is bonded to the tower (or main grounding system) using the 600mm long 16mm^2, #6AWG cable supplied in the accessory kit.

Protection requirements for a mast or tower installation

> **NOTE**
> Applies to ODU deployments only.

For equipment (ODU or antenna) mounted on a metal tower or mast, ensure that the installation meets the following requirements:

- The equipment is lower than the top of the tower or its lightning terminal and finial.
- The metal tower or mast is correctly grounded.
- A grounding kit is installed at the first point of contact between the IF cable and the tower, near the top.
- A grounding kit is installed at the bottom of the tower, near the vertical to horizontal transition point. This grounding kit is bonded to the tower or tower ground bus bar (TGB) if installed.
- If the tower is greater than 61 m (200 ft) in height, an additional grounding kit is installed at the tower midpoint. Additional ground kits are installed as necessary to reduce the distance between ground kits to 61 m (200 ft) or less.
- In high lightning prone geographical areas, additional ground kits are installed at spacing between 15 to 22 m (50 to 75 ft). This is especially important on towers taller than 45 m (150 ft).

Mast or tower protection diagrams

Figure 43 shows the protection requirements for an ODU mounted on a metal tower or mast.

Figure 44 shows the protection requirements for a 1+1 Hot Standby protected end.

Figure 43 Grounding and lightning protection on mast or tower

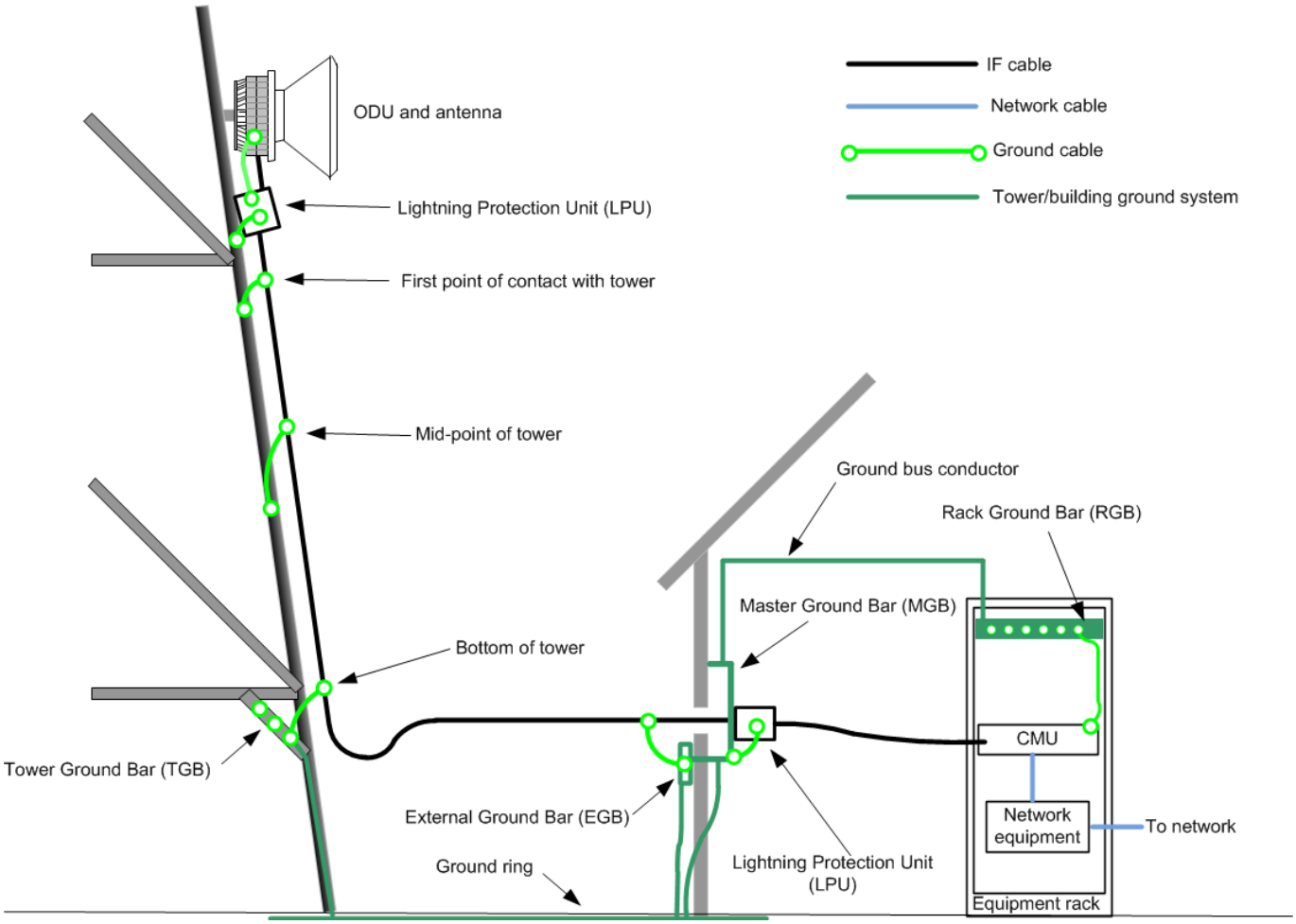
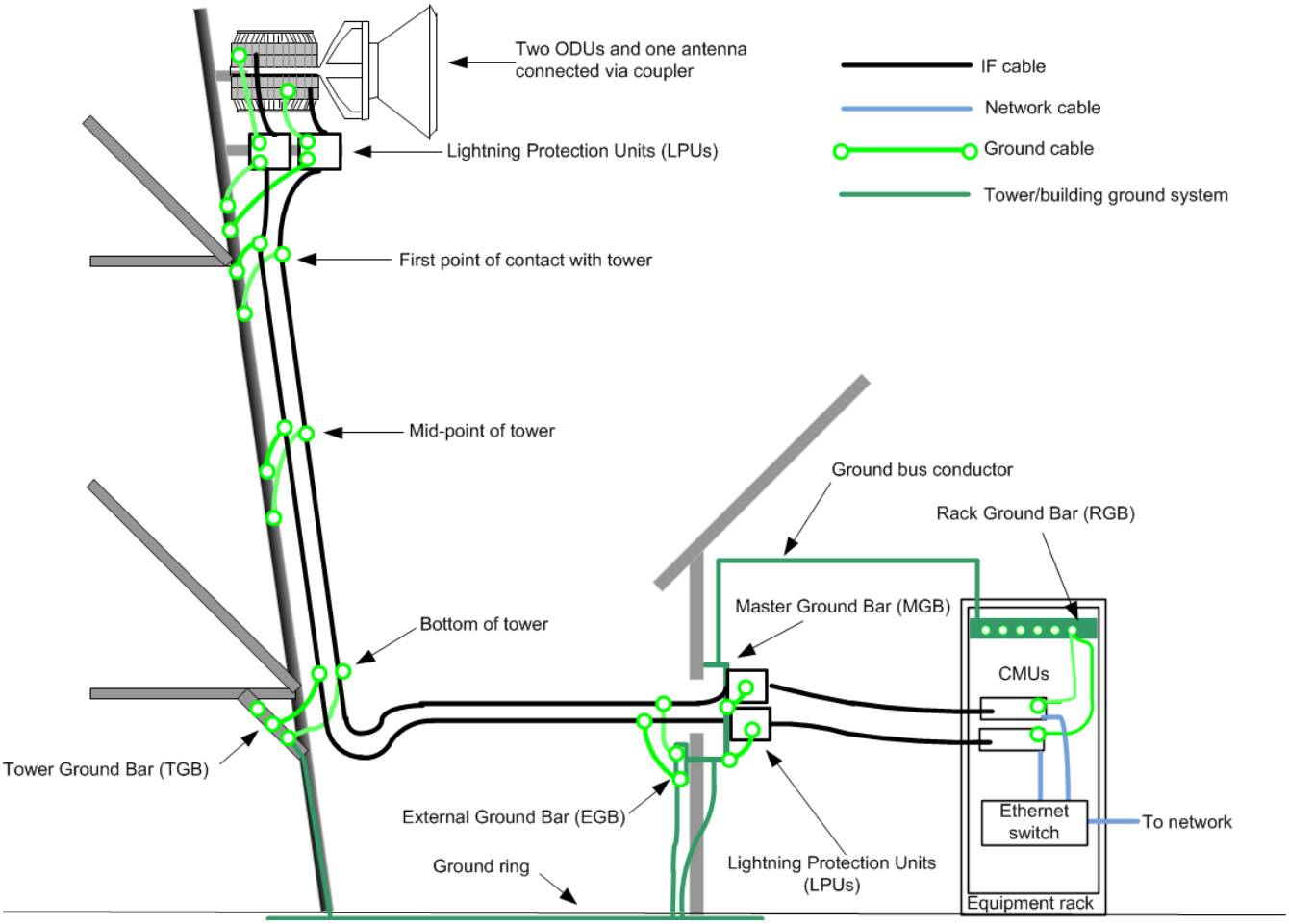


Figure 44 Grounding and lightning protection on mast or tower (protected end)



Protection requirements for the ODU on a high rise building

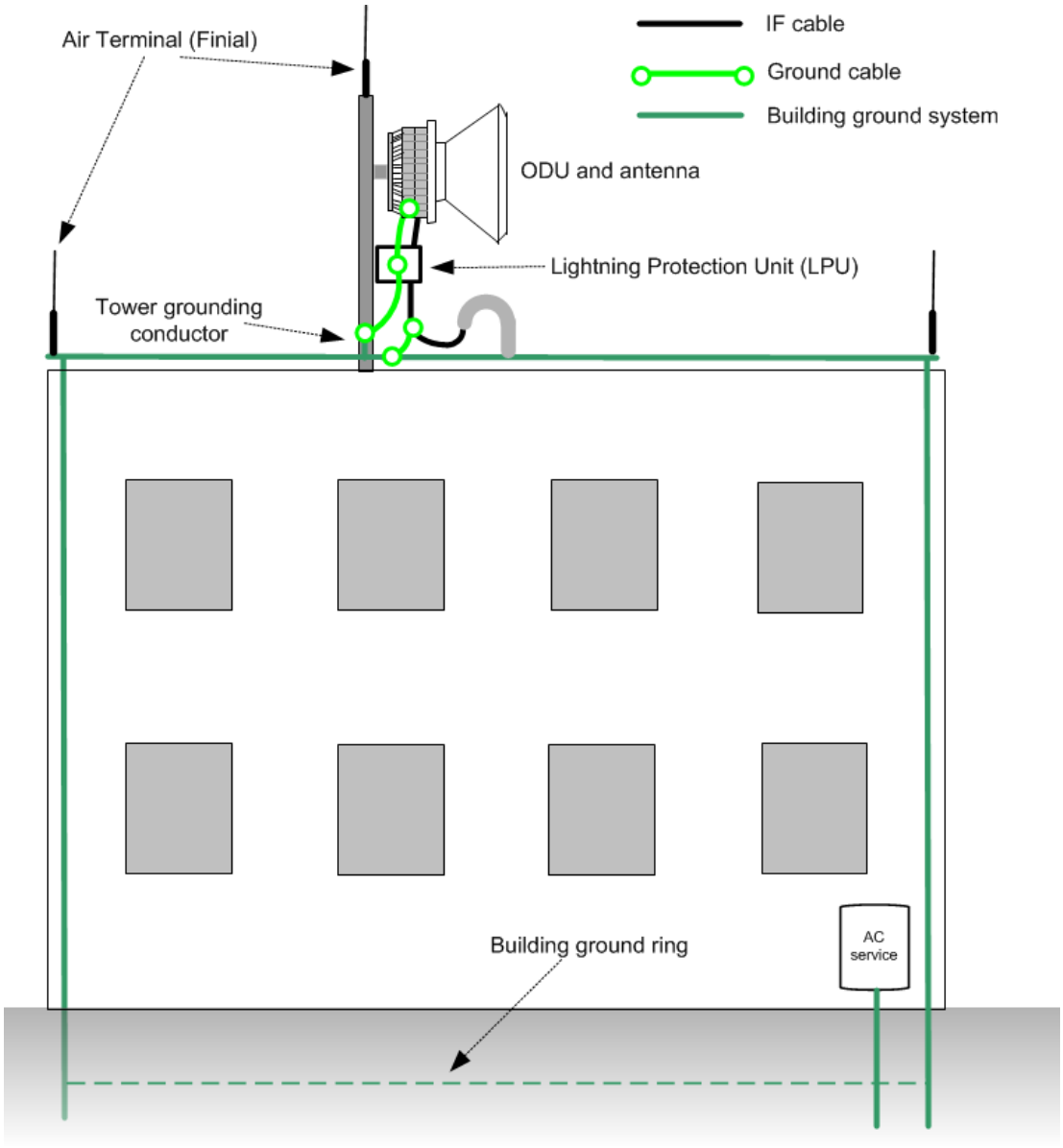
> **NOTE**
> Applies to ODU deployments only.

If the antenna or ODU is mounted on a high rise building, with cable entry at roof level (Figure 45) and the equipment inside (Figure 46), then ensure that the installation meets the following requirements:

- The antenna and ODU are below the lightning terminals and finials.
- A grounding conductor is installed around the roof perimeter, to form the main roof perimeter lightning protection ring.
- Air terminals are installed along the length of the main roof perimeter lightning protection ring typically every 6.1m (20ft).

- The main roof perimeter lightning protection ring contains at least two down conductors connected to the grounding electrode system. The down conductors are physically separated from one another, as far as practical.

Figure 45 Grounding and lightning protection on building

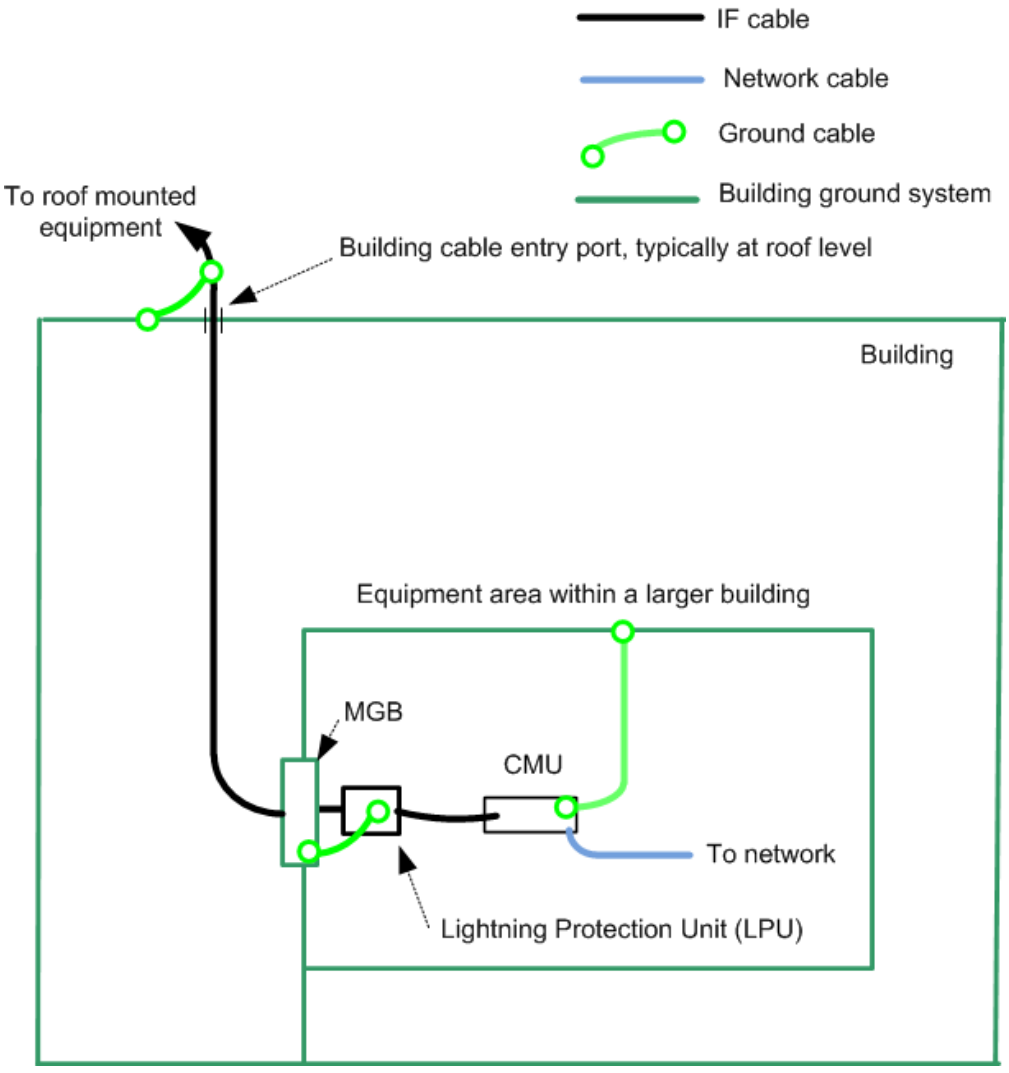


Protection inside the building

Inside multi-story or high rise buildings (Figure 46), ensure that the installation meets the following requirements:

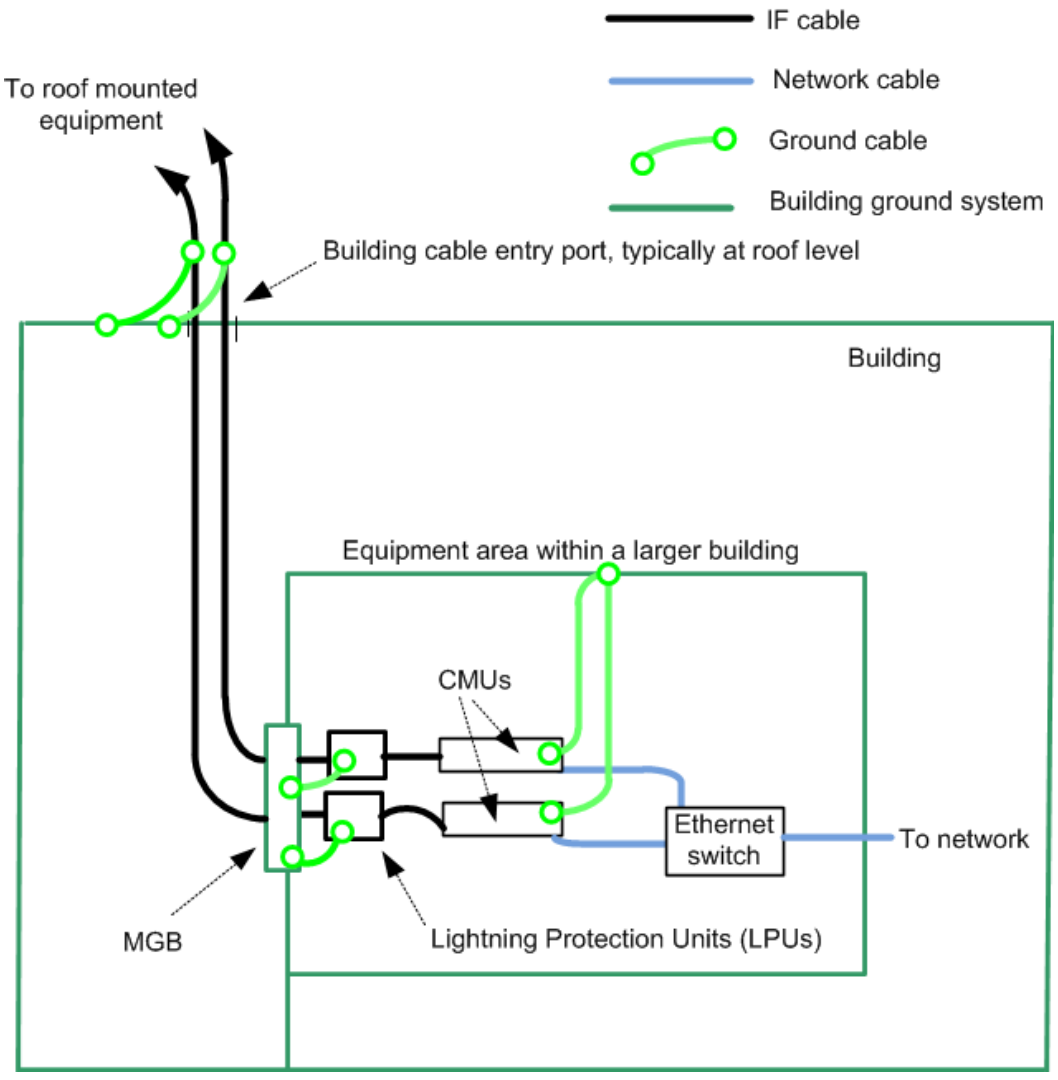
- The IF cable shield is bonded to the building grounding system at the entry point to the building.
- The IF cable shield is bonded to the building grounding system at the entry point to the equipment area.
- An LPU is installed within 600 mm (24 in) of the entry point to the equipment area.

Figure 46 Grounding and lightning protection inside high building



In a 1+1 Hot Standby protected end, prior to connecting CMUs via the protection interface, connect the front panel ground stud of both CMUs to a common ground (Figure 47).

Figure 47 Grounding and lightning protection inside high building (protected end)



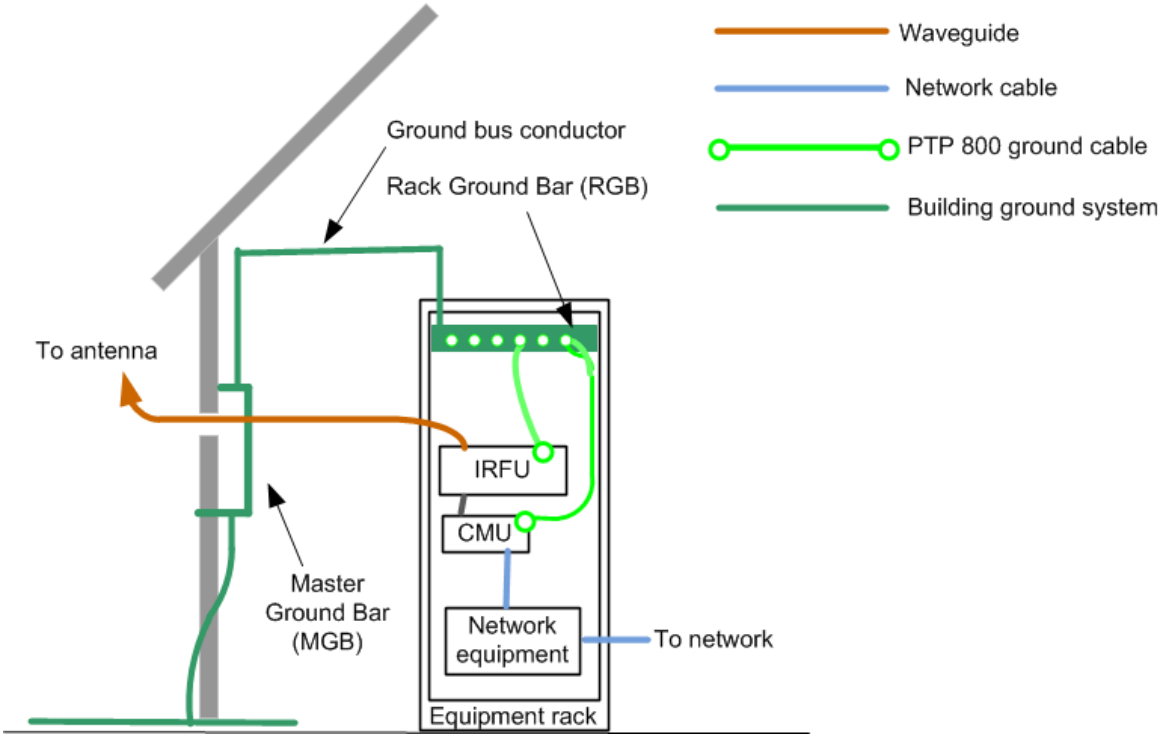
Protection requirements for the IRFU

> **NOTE**
> Applies to IRFU deployments only.

Ensure that all IRFU installations meet the following requirements:

- The CMU and IRFU are grounded at their chassis bonding points to the building grounding system (Figure 48).
- The waveguide and antenna are grounded according to their manufacturers' instructions.

Figure 48 Grounding requirements for the IRFU and CMU



Data network planning

When planning PTP 800 data networks, consider the factors described in this section.

Management mode

Decide how the PTP 800 will be managed. There are three modes of management: out-of-band local, out-of-band and in-band.

In the default out-of-band local management mode, the management agent can be reached only from the Management port of the CMU. This mode is appropriate during configuration and installation when the equipment is managed using a locally connected PC at each end of the link. It may additionally be useful where network management communication is based on a completely independent data network (for example, one based on a 3G cellular wireless terminal at each site).

In many network applications the wireless link will provide the only communication path to a remote site. In such applications, CMUs and other network equipment at the remote site will be managed over the wireless link. For applications of this type, select either out-of-band or in-band management mode.

Configure out-of-band management when there is a requirement to fully separate customer data traffic from the traffic generated by management of the network equipment. When configured for out-of-band management mode, the PTP 800 supports two networks, the customer data network and the management network. The customer data is transported between the Data ports of the CMUs and the management traffic is transported between the Management ports. The CMU management agent is also part of the management network. Traffic never crosses between the two networks. The management network has a configurable Committed Information Rate of between 100 kbps and 2 Mbps. It will also provide a maximum of 10 Mbps when there is no customer traffic to send over the link.

When configured for in-band management mode, the PTP 800 only supports a single network. Customer traffic and Management traffic are multiplexed and passed between the Data ports of the CMUs. The CMU Management port is disabled in this mode. This mode of operation may be useful where a customer has a limited number of Ethernet ports at a site.

Make sure that the same management mode is selected for CMUs at both ends of a link. See Management network on page 1-43 for further explanation of management modes.

NOTE

When using out-of-band management mode, avoid connecting Management and Data ports in the same network. Loops in the network can be complicated to detect and correct.

VLAN membership

Decide if the IP interface of the CMU management agent will be connected in a VLAN. If so, decide if this is a standard (IEEE 802.1Q) VLAN or provider bridged (IEEE 802.1ad) VLAN, and select the VLAN ID for this VLAN.

Use of a separate management VLAN is strongly recommended for applications based on the in-band management mode. Use of the management VLAN helps to ensure that the CMU management agent cannot be accessed by customers.

See Management network on page 1-43 for further explanation of VLAN membership.

Priority for management traffic

Choose the Ethernet priority for management traffic generated within the CMU management agent. Select a priority that is consistent with existing policy on priority of management traffic in the network. For in-band management, use a high priority, as this will ensure that management traffic is not discarded if the link is overloaded.

IP interface

Choose an IP address for the IP interface of the CMU management agent. The IP address must be unique and valid for the connected network segment and VLAN. Find out the correct subnet mask and gateway IP address for this network segment and VLAN.

Ensure that the design of the data network permits bi-direction routing of IP datagrams between network management systems and the CMUs. For example, ensure that the gateway IP address identifies a router or other gateway that provides access to the rest of the data network.

See Management network on page 1-43 for further explanation of configuration of the IP interface.

Quality of service for bridged Ethernet traffic

Decide how quality of service will be configured in PTP 800 to minimize frame loss and latency for high priority traffic. Wireless links often have lower data capacity than wired links or network equipment like switches and routers, and quality of service configuration is most critical at network bottlenecks.

PTP 800 provides eight queues for traffic waiting for transmission over the wireless link. Q0 is the lowest priority queue and Q7 is the highest priority queue. Traffic is scheduled using strict priority; in other words, traffic in a given queue is transmitted when all higher priority queues are empty.

Layer 2 control protocols

Select the transmission queue for each of the recognized layer 2 control protocols (L2CP). These protocols are essential to correct operation of the Ethernet network, and are normally mapped to a high priority queue. Ethernet frames that match one of the recognized L2CPs are not subject to the Ethernet and IP/MPLS classification described below.

Priority schemes

Select the priority scheme based on Ethernet priority or IP/MPLS priority to match QoS policy in the rest of the data network. Ethernet priority is also known as Layer 2 or link layer priority. IP/MPLS priority is also known as Layer 3 or network layer priority.

Ethernet priority scheme

Ethernet priority is encoded in a VLAN tag. Use the Ethernet priority scheme if the network carries traffic in customer or service provider VLANs, and the priority in the VLAN tag has been set to indicate the priority of each type of traffic. Select a suitable mapping from the Ethernet priority to the eight PTP 800 queues.

An advantage of Ethernet priority is that any VLAN-tagged frame can be marked with a priority, regardless of the higher-layer protocols contained within the frame. A disadvantage of Ethernet priority is that the priority in the frame must be regenerated whenever traffic passes through a router.

The user interface provides a convenient shortcut to select the assignment recommended in IEEE 802.1Q-2005.

IP/MPLS priority scheme

IP priority is encoded in the DSCP field in an IPv4 or IPv6 header. The DSCP field provides 64 levels of priority. Determine the DSCP values used in the network and select a suitable mapping from these DSCP values to the eight PTP 800 queues.

An advantage of IP priority is that priority in the IP header is normally propagated transparently through a router. Also, the DSCP field supports a large number of distinct priority code points. A disadvantage of DSCP is that frames receive a single default classification if they contain a network layer protocol other than IPv4 or IPv6.

MPLS priority is encoded in the traffic class (TC) field in the outermost MPLS label. Select a suitable mapping from MPLS TC to the eight PTP 800 queues.

Hot Standby links

In a 1+1 Hot Standby link, set the same QoS configuration on primary and secondary units.

Out-of-band management

When the wireless link is configured for out-of-band management, select an appropriate setting for the Management CIR attribute. A high CIR will provide greater capacity for management traffic, at the cost of allowing bursty management traffic to have a greater impact on capacity remaining for customer traffic. A low CIR may result in extended response times for network management traffic.

Fast Ethernet port shutdown

If the PTP 800 link is part of a redundant network where STP or EAPS is used in external Ethernet bridges in order to resolve loops, enable the Data Port Wireless Down Alert and Management Data Port Wireless Down Alert to ensure that protection protocols are invoked promptly following loss of the wireless link.

Security planning

When planning PTP 800 links to operate in secure mode, follow the process described in this section.

Planning for SNTP operation

To prepare for Simple Network Time Protocol (SNTP) operation:

- Identify the time zone and daylight saving requirements that apply to the system.
- Determine whether or not there is a requirement to synchronize the PTP 800 clock with an SNTP server at regular intervals. If SNTP server synchronization is not required, the clock can be set to run manually. The clock is battery backed and will continue to operate for several days after the CMU is switched off.
- If SNTP server synchronization is required, identify the details of one or two SNTP servers: IP address and server key.
- For secure applications, the PTP 800 can be configured to authenticate received NTP messages using the DES or MD5 protocols.

Planning for AES encryption

To prepare for wireless link encryption:

- Choose 128-bit or 256-bit AES encryption.
- Use a cryptographic key generator to generate an encryption key for AES. The key length is dictated by the selected AES encryption algorithm (128 or 256 bits). The same encryption key is required at each link end.

Planning for HTTPS/TLS operation

To prepare for HTTPS/TLS operation, obtain the cryptographic material listed in Table 8.

Table 8 HTTPS/TLS security material

Item	Description	Quantity required
Key of Keys	An encryption key generated using a cryptographic key generator. The key length is dictated by the installed license key. License keys with AES-128 will require a key of keys of 128-bits. License keys with AES-256 will require a key of keys of 256-bits. The key output should be in ASCII hexadecimal characters.	One per unit.
TLS Private Key and Public Certificates	An RSA private key of size 1024, generated in either PKCS#1 or PKCS#5 format, unencrypted, and encoded in the ASN.1 DER format. An X.509 certificate containing an RSA public key, generated in either PKCS#1 or PKCS#5 format, unencrypted, and encoded in the ASN.1 DER format. The public key certificate must form a valid pair with the private key.	One pair per unit.
User Defined Security Banner	The banner provides warnings and notices to be read by the user before logging in to the CMU. Use text that is appropriate to the network security policy.	Normally one per link. This depends upon network policy.
Entropy Input	This must be of size 512 bits (128 hexadecimal characters), output from a random number generator.	One per unit.
Port numbers for HTTP, HTTPS and Telnet	Port numbers allocated by the network.	As allocated by network.

Planning for FIPS 140-2 operation

To prepare for FIPS 140-2 secure mode operation, generate the following cryptographic material using a FIPS-approved cryptographic generator:

- Key of Keys
- TLS Private Key and Public Certificates. FIPS 140-2 now recommends 2048 bit keys.
- Entropy Input
- Wireless Link Encryption Key for AES

Enable the web browsers for HTTPS/TLS operation using FIPS-approved cipher specifications.

Configure the following attributes of user accounts for the web-based management interface to match the network security policy:

- Auto Logout Period.
- Maximum Number of Login Attempts.
- Login Attempt Lockout.
- Minimum Password Change Period.
- Password Expiry Period.
- Webpage Session Control

Configure the following attributes:

- Password complexity rules reset to ‘best practice’ values.
- User account passwords compliant with the network security policy.
- RADIUS authentication = Disabled.

⚠ CAUTION

Configure all of the above correctly to ensure that PTP 800 is operating in compliance with the FIPS 140-2 validation.

FIPS validated software is available from System Release PTP800-04-00. Load standard (non-FIPS) software from PTP800-04-00 or later before loading a FIPS software image.

Planning for SNMPv3 operation

SNMP security mode

Select one of the following SNMPv3 security modes:

- Use MIB-based security management to tailor views and security levels appropriate for different types of user. MIB-based security management uses standard SNMPv3 MIBs to configure the user-based security model and the view-based access control model. MIB-based security management can take advantage of the built-in security management capabilities of existing network managers.
- Use web-based security management to configure users, security levels, passphrases, and privacy and authentication protocols. The capabilities supported are somewhat less flexible than those supported using the MIB-based security management, but will be sufficient in many applications.

The system does not support concurrent use of MIB-based and web-based management.

Web-based management of SNMPv3 security

Select one of the following formats for SNMP Engine ID:

- MAC address (default).
- IP address.
- Text string: Use a string that is approved for the network management system. This is often based on some identifier that survives replacement of the PTP hardware.

HTTP and HTTPS/TLS user accounts may be assigned one of three security roles: Security Officer, System Administrator or Read Only. Initially, the PTP 800 software allows only Security Officer users to configure SNMPv3 security.

Decide whether or not that System Administrator users will be allowed to configure SNMPv3 security.

Assign a user name and security role (System Administrator or Read Only) to each SNMPv3 user.

For each security role (System Administrator and Read Only), select one of the following security levels:

- No authentication, no privacy
- Authentication, no privacy
- Authentication, privacy

Select one of the following authentication protocols (if required):

- MD5

- SHA

Select one of the following privacy protocols (if required):

- DES
- AES: This is only available to users who have purchased an appropriate license key.

For authentication and privacy protocols, identify passphrases for each protocol for each SNMP user. Use different passphrases for authentication and privacy. Passphrase length is between 8 and 32 characters, with the permitted characters listed in Table 9.

Table 9 Permitted character set for SNMPv3 passphrases

Character	Code	Character	Code
<space>	32	;	59
!	33	<	60
“	34	=	61
#	35	>	62
$	36	?	63
%	37	@	64
&	38	A..Z	65..90
'	39	[	91
(	40	\	92
)	41	]	93
*	42	^	94
+	43	_	95
,	44	`	96
-	45	a..z	97..122
.	46	{	123
/	47	|	124
0..9	48..57	}	125
:	58	~	126

Identify up to two SNMP users that will be configured to receive notifications (traps). Identify the IP address and UDP port number of the associated SNMP manager.

SNMPv3 default configuration (MIB-based)

When SNMPv3 MIB-based Security Mode is enabled, the default configuration for the `usmUserTable` table is based on one initial user and four template users as listed in Table 10.

Table 10 Default SNMPv3 users

Object	Entry 1	Entry 2	Entry 3
Name	initial	templateMD5_DES	templateSHA_DES
SecurityName	initial	templateMD5_DES	templateSHA_DES
AuthProtocol	usmHMACMD5AuthProtocol	usmHMACMD5AuthProtocol	usmHMACSAHAuthProtocol
PrivProtocol	usmDESPrivProtocol	usmDESPrivProtocol	usmDESPrivProtocol
StorageType	nonVolatile	nonVolatile	nonVolatile

Object	Entry 4	Entry 5
Name	templateMD5_AES	templateSHA_AES
SecurityName	templateMD5_AES	templateSHA_AES
AuthProtocol	usmHMACMD5AuthProtocol	usmHMACSHAAuthProtocol
PrivProtocol	usmAESPrivProtocol	usmAESPrivProtocol
StorageType	nonVolatile	nonVolatile

Planning for RADIUS operation

Configure RADIUS where remote authentication is required for users of the web-based interface. Remote authentication has the following advantages:

- Control of passwords can be centralized.
- Management of user accounts can be more sophisticated For example, users can be prompted by email to change passwords at regular intervals. As another example, passwords can be checked for inclusion of dictionary words and phrases.
- Passwords can be updated without reconfiguring multiple network elements.
- User accounts can be disabled without reconfiguring multiple network elements.

Remote authentication has one significant disadvantage in a wireless link product such as PTP 800. If the wireless link is down, a unit on the remote side of the broken link may be prevented from contacting a RADIUS Server, with the result that users are unable to access the web-based interface.

One useful strategy would be to combine RADIUS authentication for normal operation with a single locally-authenticated user account for emergency use.

PTP 800 provides a choice of three authentication methods:

- CHAP
- MS-CHAPv2
- PEAP(MS-CHAPv2)

PEAP(MS-CHAPv2) is supported for Microsoft Windows Server 2003.

Ensure that the authentication method selected in PTP 800 is supported by the RADIUS server.

RADIUS is not permitted in FIPS 140-2 applications. RADIUS and PEAP(MS-CHAPv2) are mandatory in UC-APL applications.

RADIUS attributes

If the standard RADIUS attribute session-timeout (Type 27) is present in a RADIUS response, PTP 800 sets a maximum session length for the authenticated user. If the attribute is absent, the maximum session length is infinite.

If the standard RADIUS attribute idle-timeout (Type 28) is present in a RADIUS response, PTP 800 overrides the Auto Logout Timer with this value in the authenticated session.

If the vendor-specific RADIUS attribute auth-role is present in a RADIUS response, PTP 800 selects the role for the authenticated user according to auth-role. The supported values of auth-role are as follows:

- 0: Invalid role. The user is not admitted.
- 1: Read Only
- 2: System Administrator
- 3: Security Officer

If the vendor-specific auth-role attribute is absent, but the standard service-type (Type 6) attribute is present, PTP 800 selects the role for the authenticated user according to service-type. The supported values of service-type are as follows:

- Login(1): Read Only
- Administrative(6): System Administrator
- NAS Prompt(7): Read Only

If the auth-role and service-type attributes are absent, PTP 800 selects the Read Only role.

The auth-role vendor-specific attribute is defined in Table 11.

Table 11 Definition of auth-role vendor-specific attribute

Field	Length	Value	Notes
Type	1	26	Vendor-specific attribute.
Length	1	12	Overall length of the attribute.
Vendor ID	4	17713	The same IANA code used for the SNMP enterprise MIB.
Vendor Type	1	1	auth-role
Vendor Length	1	4	Length of the attribute specific part.
Attribute-Specific	4	0..3	Integer type (32-bit unsigned). Supported values: invalid-role(0), readonly-role(1), system-admin-role(2), security-officer-role(3).

Planning 1+0 links

When planning 1+0 links, follow the process described in this section.

Concept of a 1+0 link

A 1+0 link is the simplest link to deploy. There is no redundant equipment deployed and so costs are minimized. The 1+0 link provides no protection in the case of equipment failure. If a link is very critical to network operation and where a service outage due to equipment failure cannot be tolerated, consider deploying a 1+1 Hot Standby link.

Antenna, RFU and CMU configurations for 1+0

Select one of the following 1+0 link end configurations:

- ODU with direct mount antenna (Figure 49).
- ODU with remote mount antenna (Figure 50).
- IRFU with remote mount antenna (Figure 51).

Do not install an ODU and an IRFU in the same link, as they cannot interwork.

Figure 49 Schematic view of 1+0 ODU direct mount link end

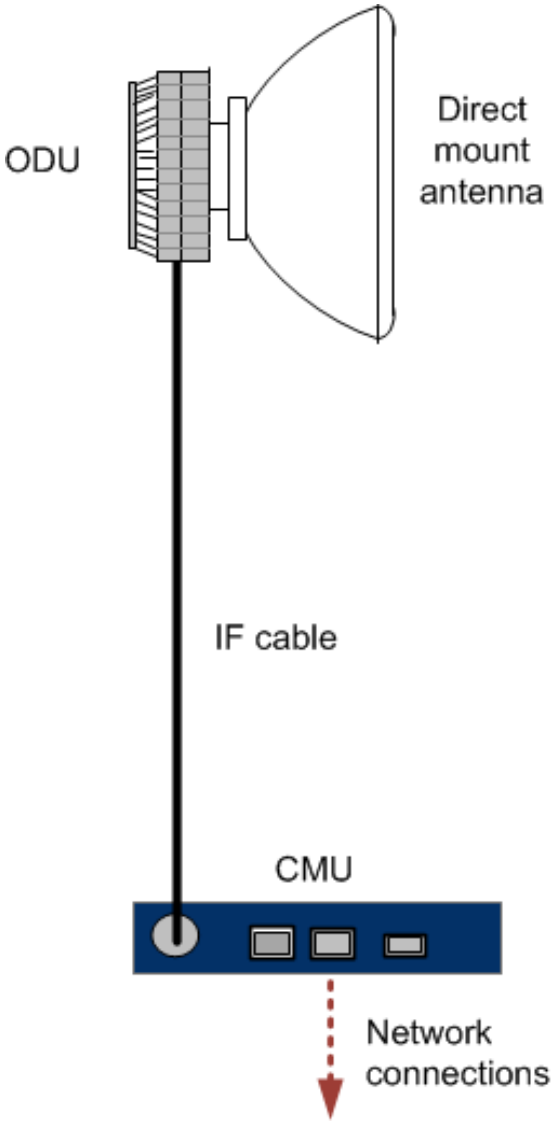


Figure 50 Schematic view of 1+0 ODU remote mount link end

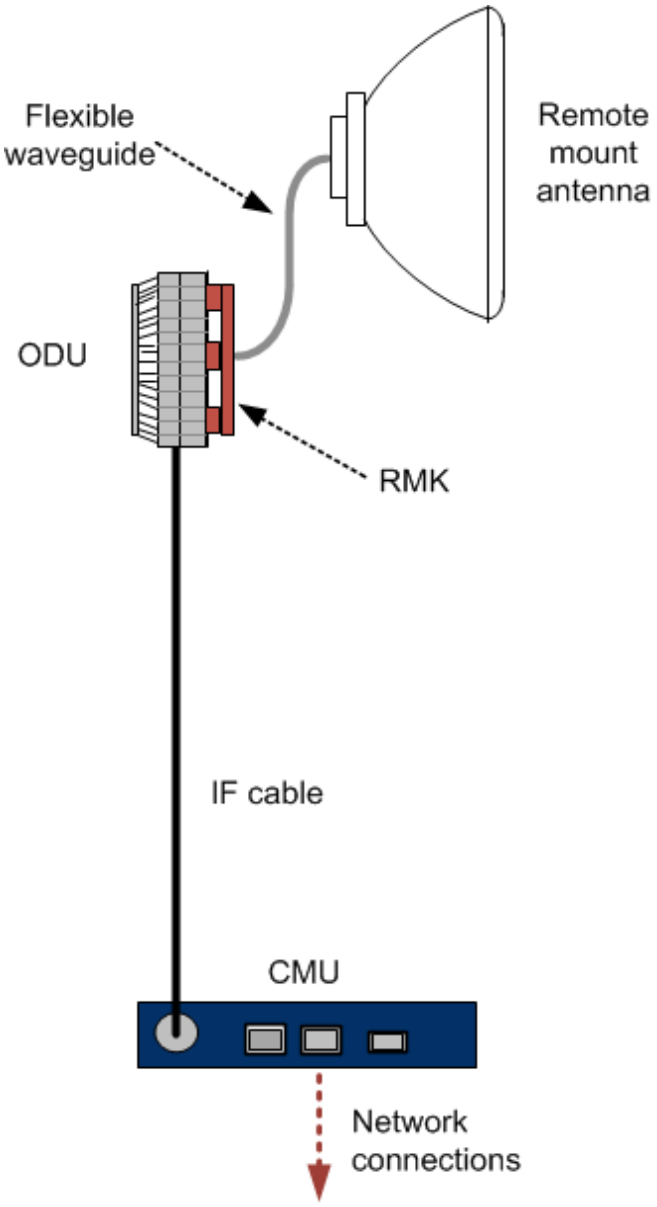
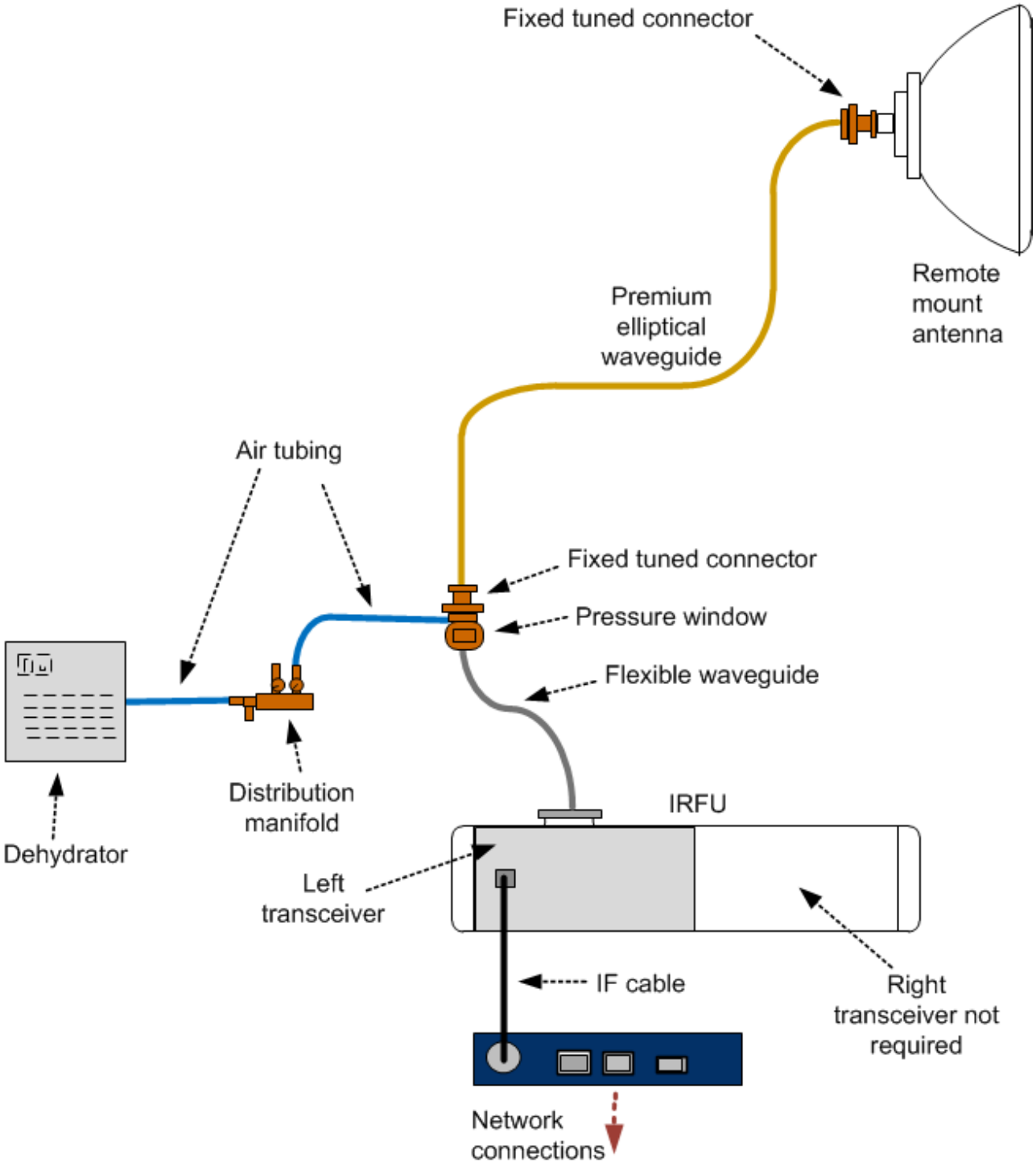


Figure 51 Schematic view of 1+0 IRFU link end

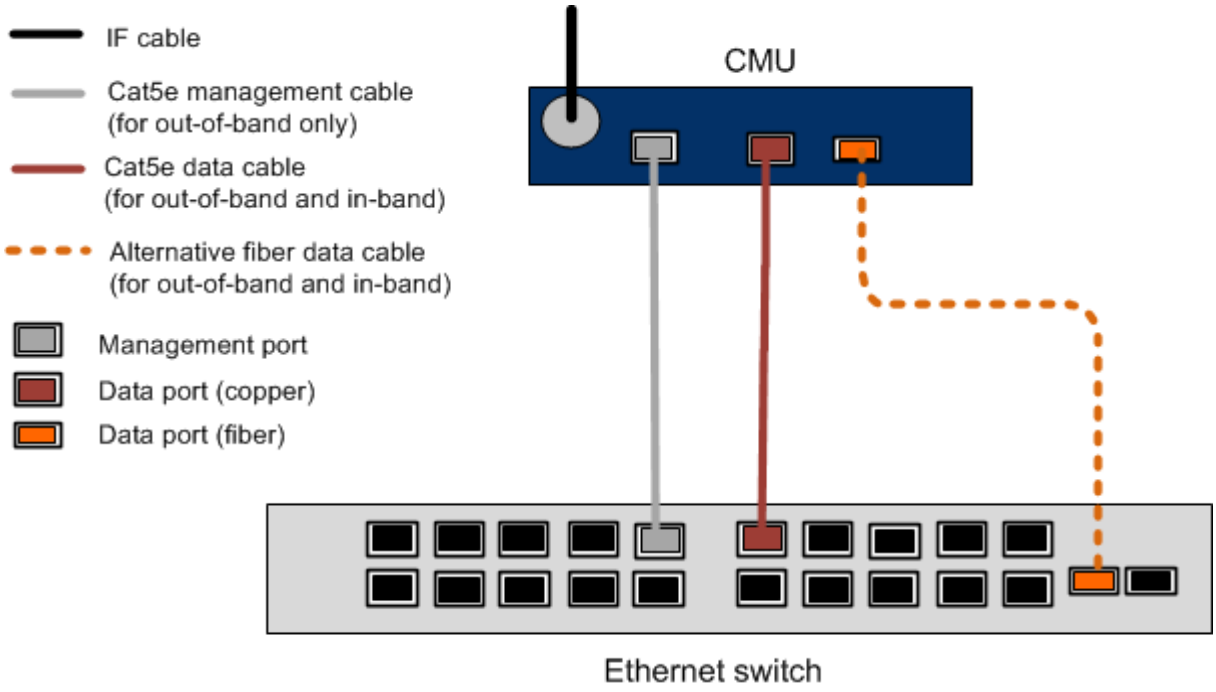


Network configurations for 1+0

Install the 1+0 network connections as shown in Figure 52. For out-of-band management, provide both Data port and Management port cables. For in-band management, provide Data port cables only.

For part numbers, see Ordering network connection components on page 2-96.

Figure 52 Schematic view of network connections for a 1+0 link end



Planning 1+1 Hot Standby links

When planning 1+1 Hot Standby links, follow the process described in this section.

Concept of a 1+1 Hot Standby link

A 1+1 Hot Standby link provides protection against single point equipment failure. This is achieved by the deployment of extra equipment which automatically takes over the operation of the link in case of failure.

The two main advantages of a 1+1 Hot Standby link are:

- Better availability. In the unlikely event of equipment failure, the 1+1 Hot Standby link becomes operational again with a down time of less than 250 ms. This is compared to a lengthy down time in the event of equipment failure in a 1+0 link. This may be particularly important in remote locations or for safety critical applications.
- Maintenance operations can be carried out, such as installation of new software, with a minimum of interruption to the service provided by the link.

Antenna, RFU and CMU configurations for 1+1

⚠ CAUTION

Do not install an ODU and an IRFU in the same link, as they cannot interwork.

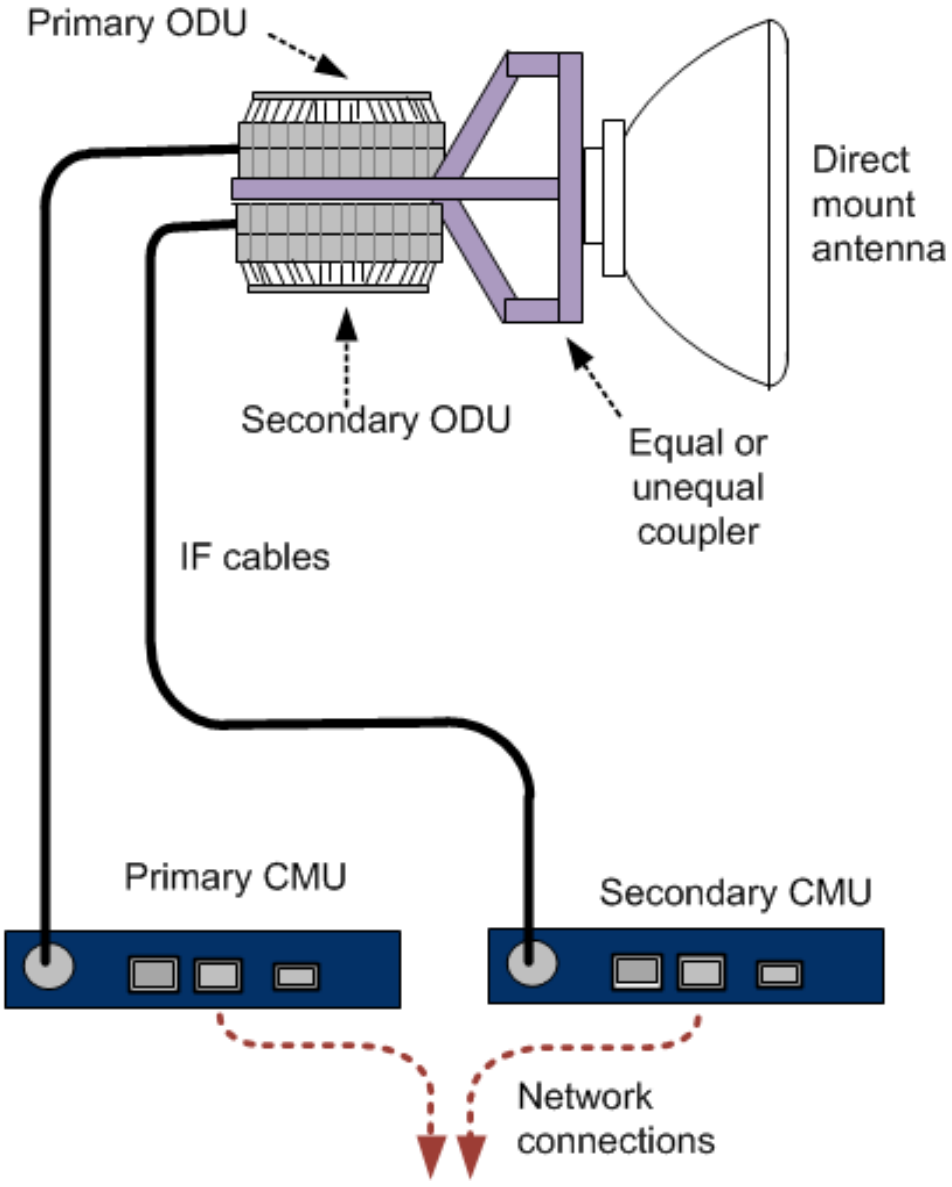
Select one of the following 1+1 Hot Standby link end configurations:

ODUs coupled to single direct mount antenna

The coupler mounts directly to the back of the antenna (Figure 53).

Choose equal or unequal couplers. The unequal coupler provides a better link budget (nominally 6 dB) for the Primary ODUs at the expense of the link budget of the Secondary ODUs.

Figure 53 ODUs coupled to single direct mount antenna (schematic)

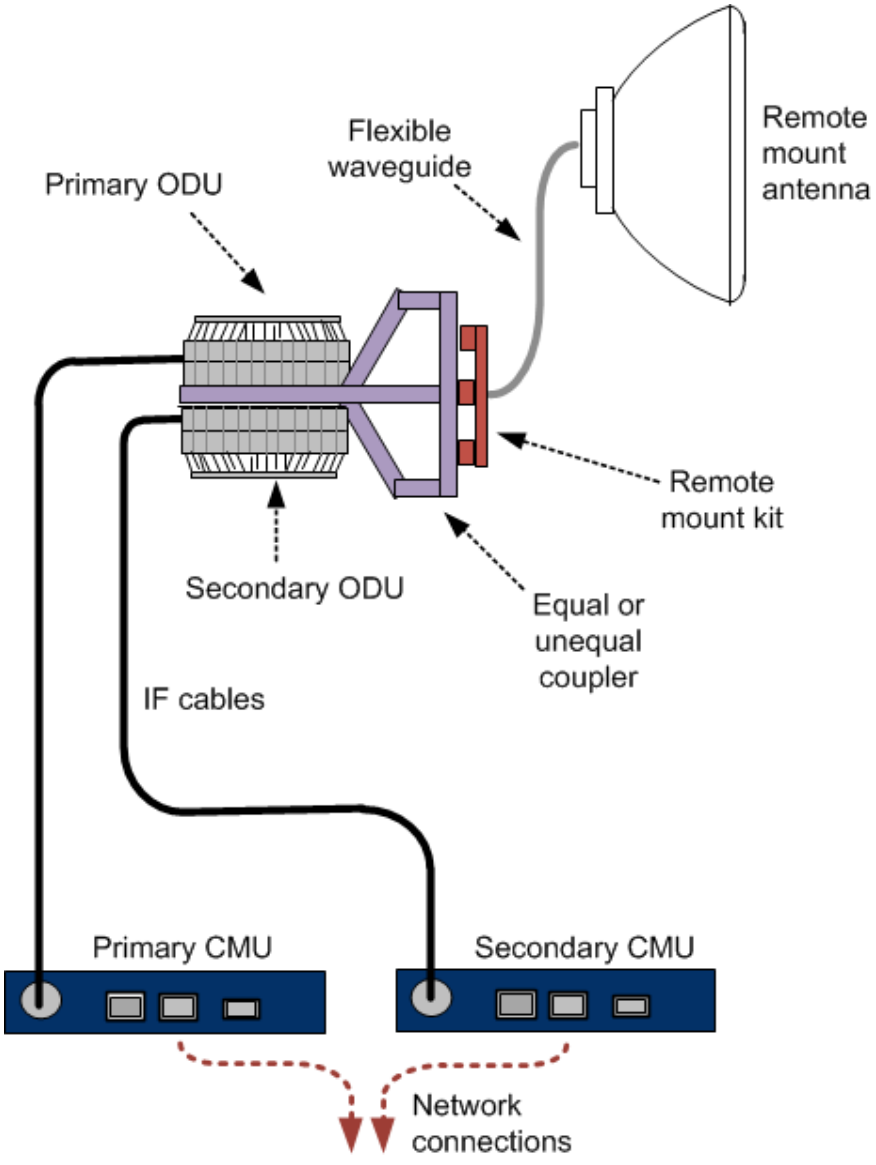


ODUs coupled to single remote mount antenna

Requires a Remote Mount Kit (RMK) to mount the Coupler and 3' of flexible waveguide to connect the RMK to the antenna (Figure 54).

Choose equal or unequal couplers. The unequal coupler provides a better link budget (nominally 6 dB) for the Primary ODUs at the expense of the link budget of the Secondary ODUs.

Figure 54 ODUs coupled to single remote mount antenna (schematic)

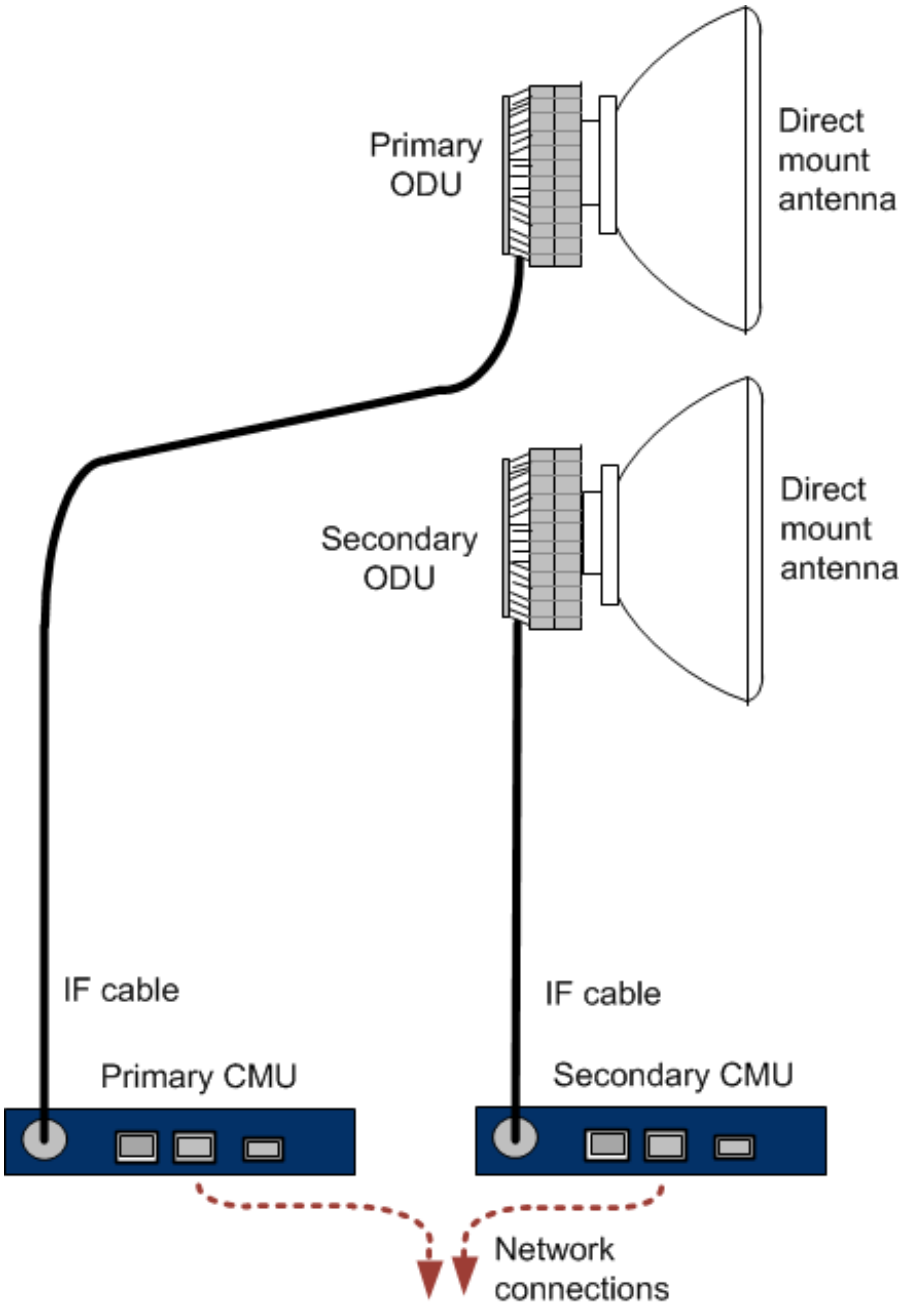


ODUs with separate direct mount antennas

May be used to provide Spatial Diversity. The ODUs mounts directly to the back of the antennas (Figure 55).

The antenna connected to the Secondary ODU may have lower gain if space on the mast is an issue. Although antennas may have different gains, the polarizations must be the same.

Figure 55 ODUs with separate direct mount antennas (schematic)

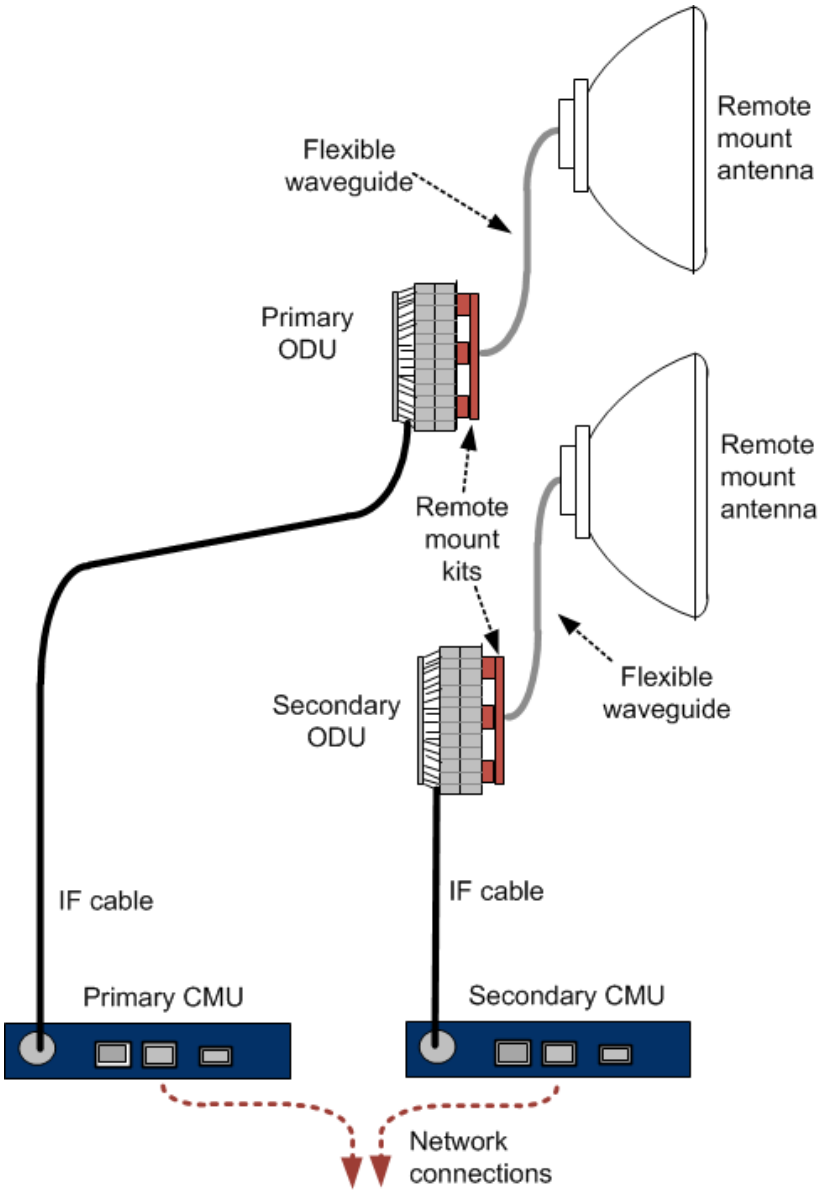


ODUs with separate remote mount antennas

May be used to provide Spatial Diversity. Each ODU is mounted using a Remote Mount Kit (Figure 56). Each RMK connects to its antenna with a 3' flexible waveguide.

The antenna connected to the Secondary ODU may have lower gain if space on the mast is an issue. Although antennas may have different gains, the polarizations must be the same.

Figure 56 ODUs with separate remote mount antennas (schematic)

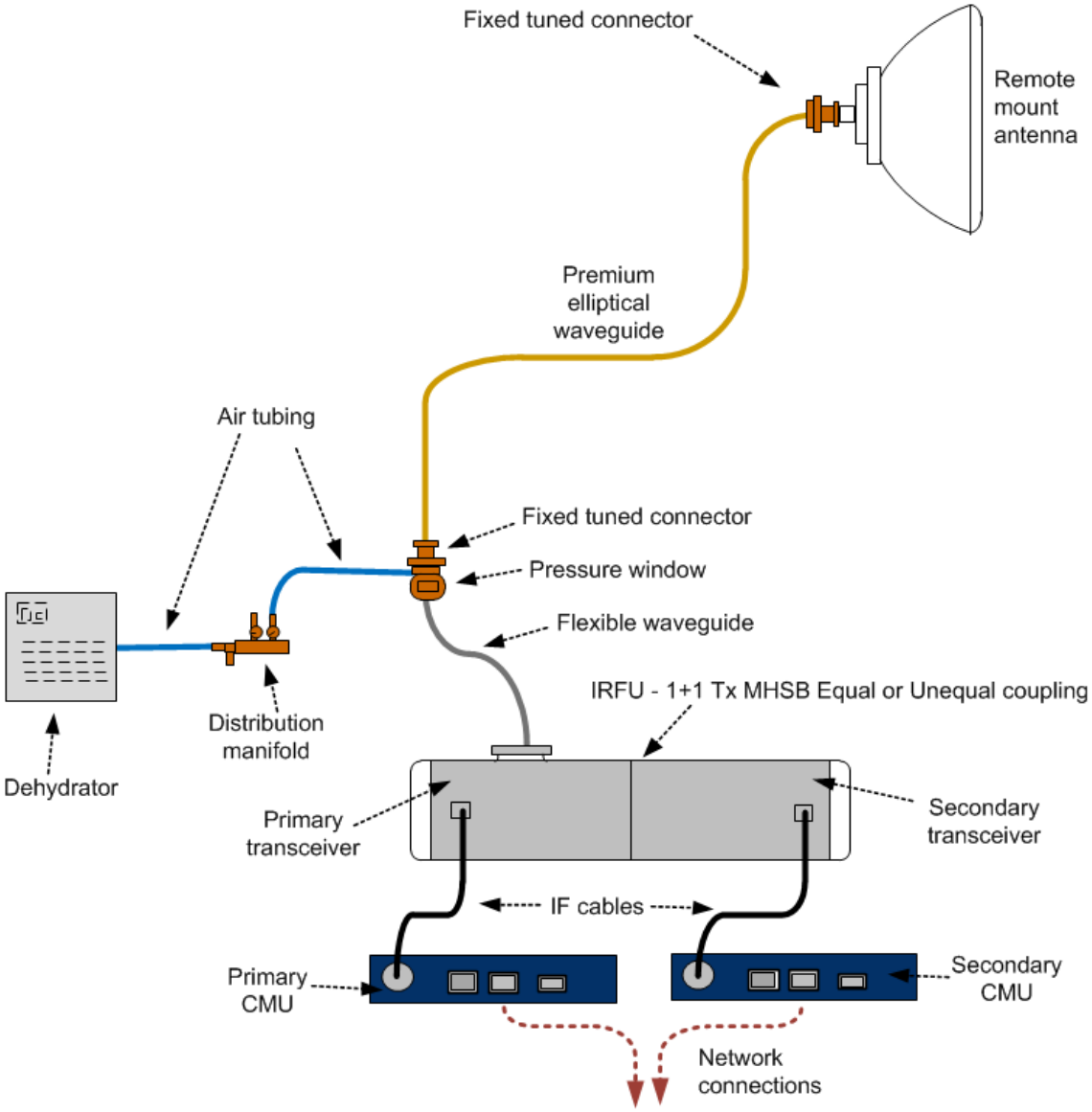


IRFU 1+1 Tx MHSB with single remote mount antenna

Requires a length of elliptical waveguide dependant on the distance between the antenna and the IRFU (Figure 57). Requires waveguide dehydration accessories. The receiver coupling is internal to the IRFU.

Choose IRFUs with equal or unequal coupling. The unequal coupling option provides a better link budget (nominally 6 dB) for the Primary transceivers.

Figure 57 IRFU 1+1 Tx MHSB with single remote mount antenna (schematic)

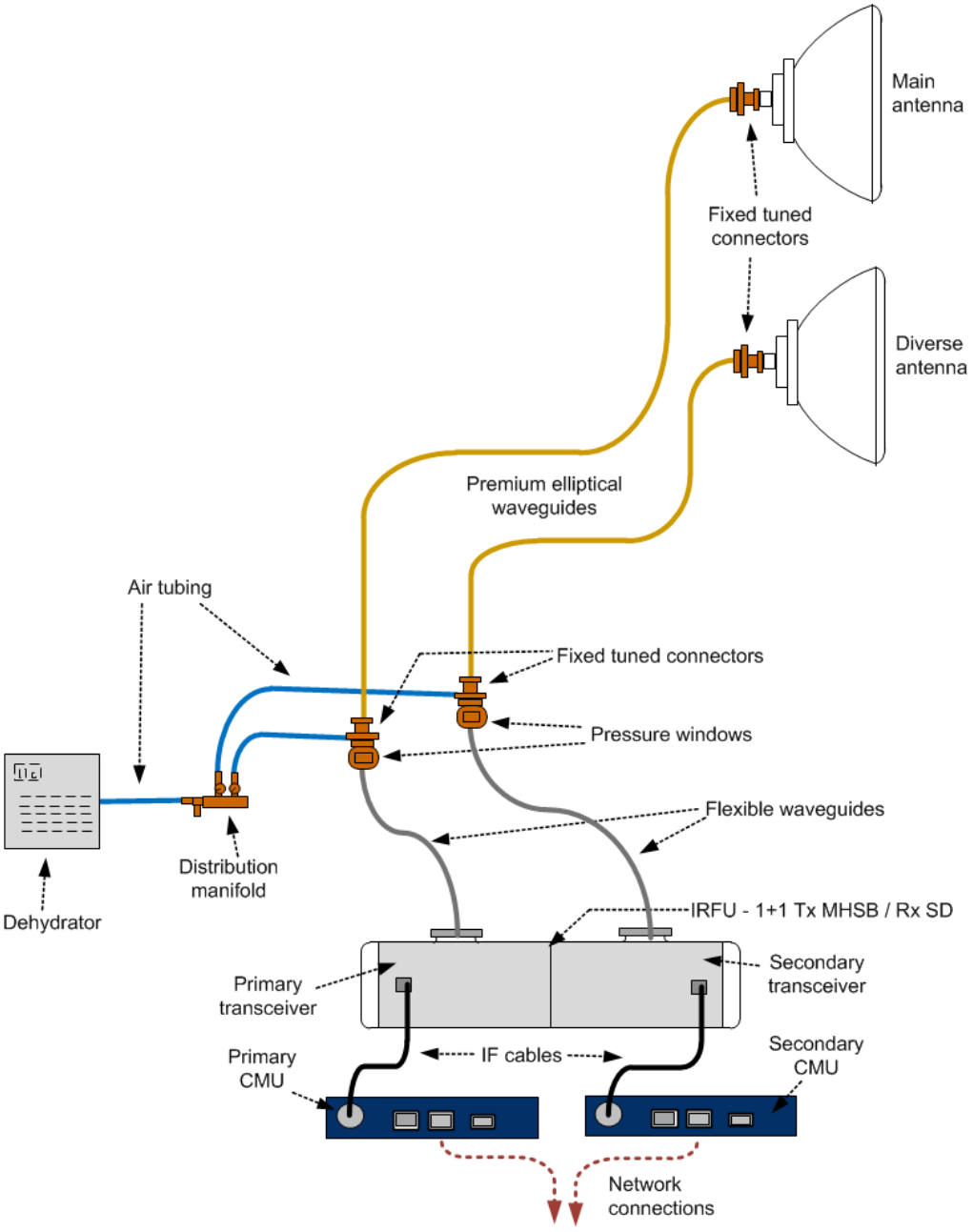


IRFU 1+1 Tx MHSB / Rx SD with two remote mount antennas

Requires two lengths of elliptical waveguide (Figure 58). The length of each waveguide is dependant on the distance between the antenna and the IRFU. Requires waveguide dehydration accessories. The IRFU will only radiate from the main antenna.

The diverse antenna may be selected with lower gain if space on the mast is an issue. Both antennas must have the same polarity.

Figure 58 IRFU 1+1 Tx MHSB / Rx SD with two remote mount antennas (schematic)



Designating primary and secondary units

At each link end, designate one unit as Primary and the other as Secondary, applying the following criteria:

- The Primary CMU is connected to the ODU or IRFU transceiver with the best link budget. In ODU deployments with unequal couplers, this is the ODU connected to the arm of the coupler with the lowest path loss. The coupler labels this arm as "Main".
- If separate antennas are deployed, the Primary CMU is connected to the ODU that is connected to the antenna with the highest gain. If equal gain antennas are used, either CMU can be configured as the Primary.
- In IRFU deployments, the Primary CMU is connected to the left hand transceiver.

The procedure for configuring the primary and secondary units is described in Configuring 1+1 Hot Standby links on page 6-54).

Link Planning for 1+1 Hot Standby links

A 1+1 Hot Standby link has four radio paths:

- Primary end A to Primary end B
- Primary end A to Secondary end B
- Secondary end A to Primary end B
- Secondary end A to Secondary end B

A 1+1 Hot Standby link normally operates on the Primary to Primary radio path. However, any of the four paths may become active if a fault causes a protection switch at one end of the link. Use LINKPlanner to check wireless link availability for all four paths, ensuring that the minimum required availability can be met by all paths.

Network configurations for 1+1

1+1 Hot Standby link management

In a 1+1 Hot Standby Link, each CMU is managed separately and must be assigned its own IP address.

Choosing Ethernet switches

The Ethernet switch must react to a brief disconnection of an Ethernet port by flushing its forwarding data base (see Bridging in 1+1 links on page 1-66). This allows the Ethernet switch to learn the new bridging path following a protection switch. When choosing an Ethernet switch, ensure that this feature is supported.

> **NOTE**
> Many inexpensive unmanaged switches fail to meet this requirement.

The switch must support the required number of ports for 1+1 Hot Standby operation. This is dependent on the following factors:

- Whether copper or fiber is the physical connection medium or whether the Fiber-Y option is required.
- Whether in-band or out-of-band management mode is required.

The details of these requirements are in the following sections.

1+1 Hot Standby link with out-of-band management

Out-of-band management provides two separate networks, one for customer data and one for managing the network. Please refer to Management network on page 1-43 for more details on out-of-band Management.

When Out of Band management is selected, the Ethernet switch must provide two ports in order to carry the management traffic to both CMUs. As the protection interface shares the same physical socket as the management port, an Out of Band Protection Splitter is required to route the management traffic from the two CMUs to the Ethernet switch.

For the customer data, there are two methods of connection, either redundant data ports or Fiber-Y.

For redundant data ports, the Ethernet switch must provide two ports for carrying customer data traffic to both CMUs. The choice of physical medium can be copper or fiber and this can be selected independently for each CMU. This arrangement is shown in Figure 59.

The Fiber-Y arrangement can be a useful feature in complex networks, such as ring architectures, where there is a requirement for the link to provide a single interface at the Ethernet Switch. The Ethernet Switch must provide a single fiber port. This arrangement is shown in Figure 60.

Figure 59 Schematic of 1+1 out-of-band network connections (redundant copper or fiber)

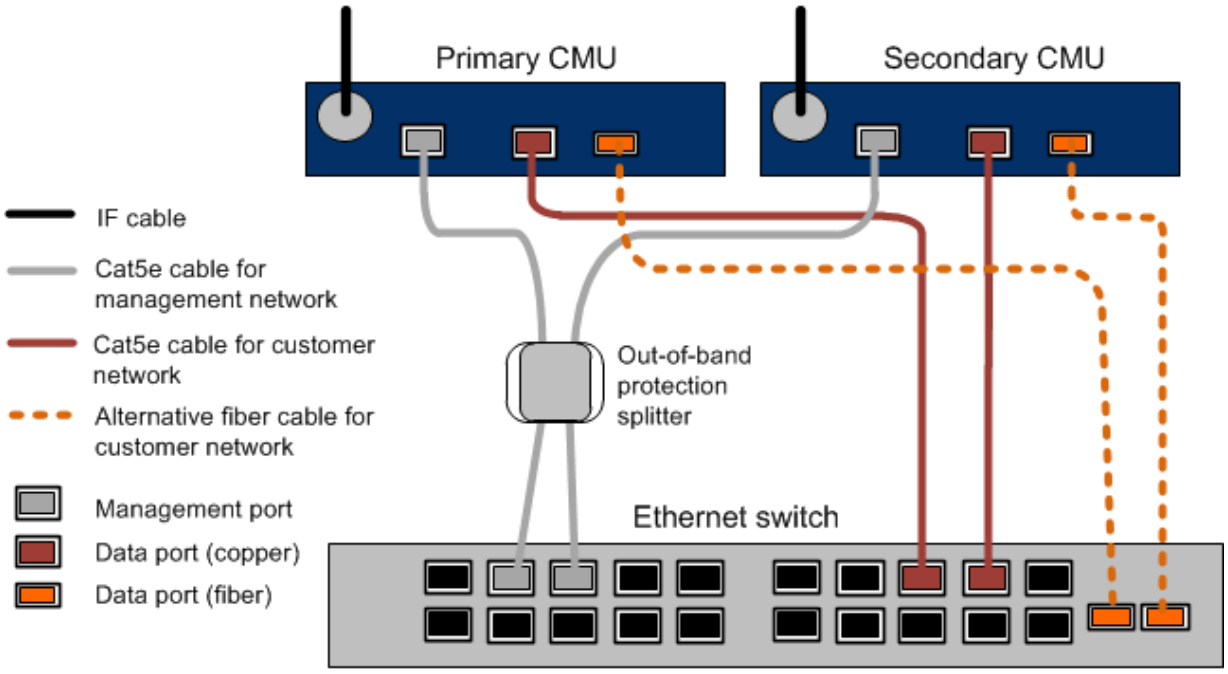
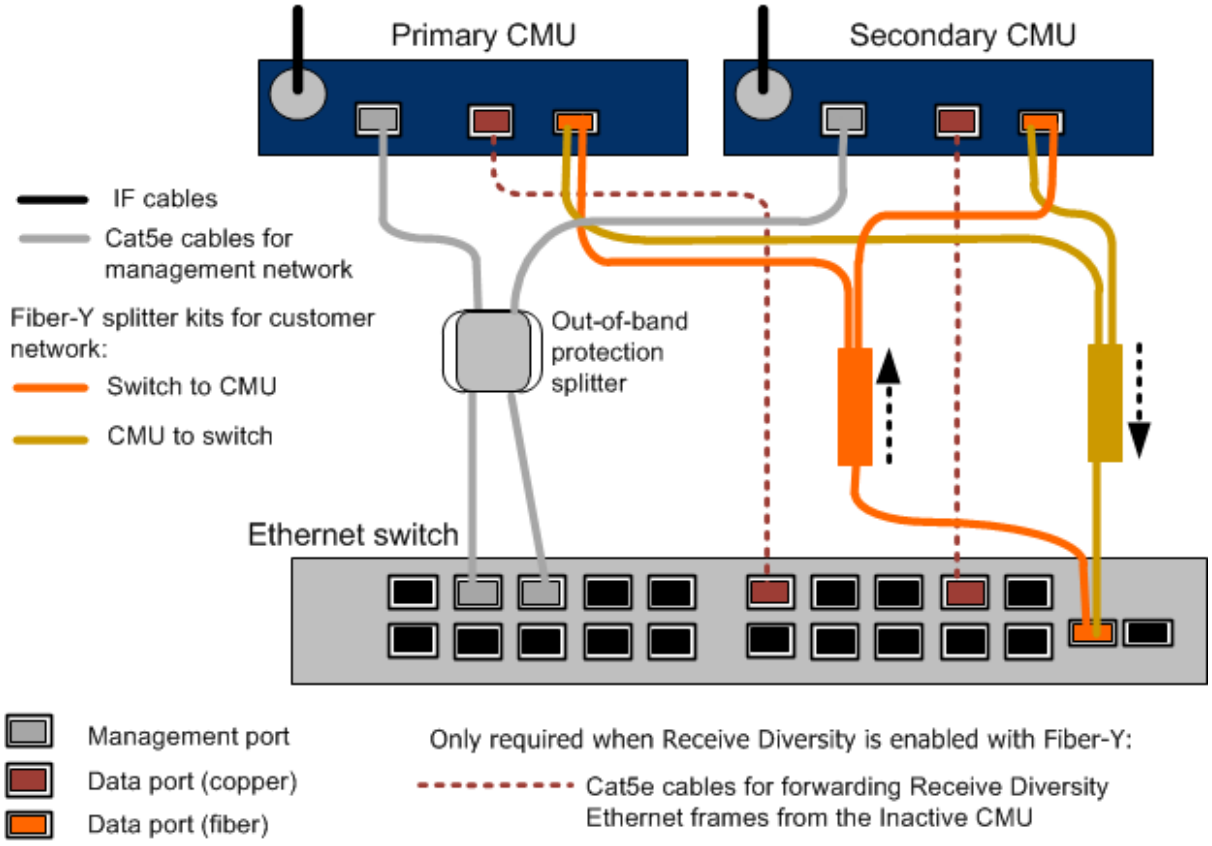


Figure 60 Schematic of 1+1 out-of-band network connections (Fiber-Y)


Primary CMU
Secondary CMU
IF cables
Cat5e cables for management network
Fiber-Y splitter kits for customer network:
Switch to CMU
CMU to switch
Out-of-band protection splitter
Ethernet switch
Management port
Data port (copper)
Data port (fiber)
Only required when Receive Diversity is enabled with Fiber-Y:
Cat5e cables for forwarding Receive Diversity Ethernet frames from the Inactive CMU

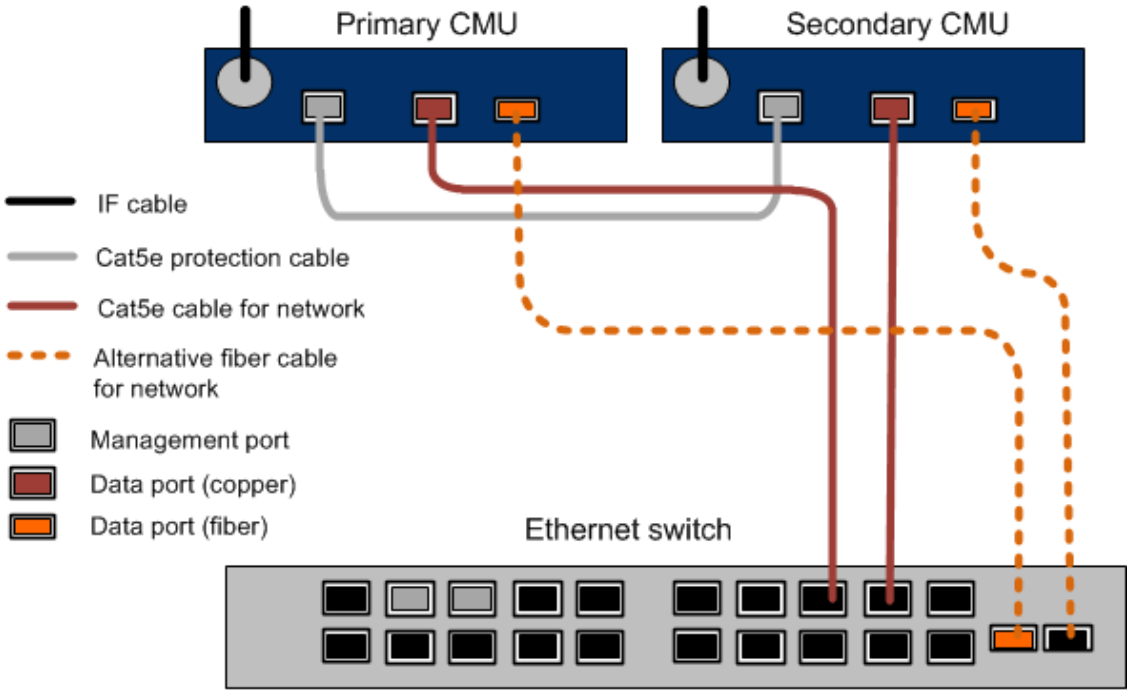
1+1 Hot Standby link with in-band management

In Band management provides a single network which multiplexes customer data with management data. Please refer to Management network on page 1-43 for more details of this mode.

When In Band is configured, the Ethernet Switch must provide two ports to carry the traffic to the two CMUs. The choice of physical medium can be copper or fiber and this can be selected independently for each CMU. This arrangement is shown in Figure 61.

For correct 1+1 Hot Standby operation, the two CMUs must also be connected together over the protection interface. Please refer to Protection cable on page 4-17.

Figure 61 Schematic of 1+1 in-band network connections



Planning for Receive Diversity

PTP 800 supports the Receive Diversity feature, which provides hitless protection against receiver faults. This feature can be enabled (at the CMU) in any of the supported 1+1 Hot Standby configurations described in Antenna, RFU and CMU configurations for 1+1 on page 2-35.

This feature provides Receive Spatial Diversity when two antennas are installed at the same end, that is, in the following configurations:

- ODUs with separate direct mount antennas on page 2-38
- ODUs with separate remote mount antennas on page 2-39
- IRFU 1+1 Tx MHSB / Rx SD with two remote mount antennas on page 2-41

For further information on the Receive Diversity feature, see Receive Diversity on page 1-67.

Ethernet Switch Requirements for Receive Diversity

In addition to the Ethernet Switch features required to support operation of a 1+1 Hot Standby link, further features are required when Receive Diversity is enabled. This is because the Ethernet Switch must bridge special Receive Diversity Ethernet Frames from the Inactive CMU to the Active CMU. The payload of these frames contains the demodulated and decoded data received at the wireless interface of the Inactive CMU. The Active CMU can then make use of the data received at the wireless interface of either CMU.

- The customer data ports which connect the Ethernet Switch to the CMU must be capable of negotiating at 1 Gbps full duplex. This is to ensure that latency is kept to a minimum and that the highest capacity configurations can be supported. Note that Receive Diversity Frames are not sent from the Inactive CMU if either CMU has trained at less than 1 Gbps full duplex.
- The Ethernet Switch must support the configuration of Virtual LANs using either 802.1Q or 802.1ad. Configuring a dedicated VLAN to bridge Receive Diversity Ethernet Frames from the Inactive CMU to the Active CMU prevents these frames from flooding the network.
- The network configurations are identical to those described for the 1+1 Hot Standby configurations (see Network configurations for 1+1 on page 2-43), with the exception of the Fiber-Y configuration. In addition to connecting the Fiber ports of the CMU to the Ethernet switch using Fiber-Y, the copper data ports of the CMUs must also connect to the Ethernet switch (see Figure 60). The copper data port will only be used for forwarding Receive Diversity Frames out of the Inactive CMU which will necessarily have its fiber port disabled in the Fiber-Y configuration. Customer data will only ever be forwarded to and from the Fiber port of the Active CMU ensuring that the Fiber-Y configuration meets the requirement for a single customer data port at the Ethernet switch.

VLAN considerations for Receive Diversity

The ports which connect the Ethernet Switch to the CMUs must be configured into a dedicated VLAN for Receive Diversity Ethernet Frames. Only these two ports must be configured in this VLAN to prevent the frames from flooding the network. Existing VLANs configured for these ports will not be affected. The following attributes must be considered when planning for Receive Diversity.

- Select either C-TAG (802.1Q) or S-TAG (802.1ad) operation for the Receive Diversity VLAN. The configuration at the switch must match the value of the CMU attribute Rx Diversity TPID.
- Select a dedicated VLAN identifier (VID) for the Receive Diversity VLAN. The configuration at the switch must match the value of the CMU attribute Rx Diversity VID.

- At the Ethernet Switch, configure the Receive Diversity VLAN for tagged operation. At the ingress, the ports in this VLAN must accept tagged frames which arrive with the Receive Diversity VID and forward them to the other port which is also a member of this VLAN. At the egress, the Ethernet Switch must NOT strip the Receive Diversity tag.

Performance considerations for Receive Diversity

As the Ethernet Switch multiplexes the Receive Diversity Frames with customer traffic, consider the impact of Receive Diversity on latency and jitter.

When the link is not fading, the maximum latency increases by 12 µs in all configurations.

When the link fades to the point where the Active unit can no longer demodulate a signal and where the data stream from the Inactive unit is being used, the maximum latency increases to a value which is dependent on the frames size of the customer traffic as shown in Table 12.

Table 12 Frame size and latency relationship in Rx SD links

Maximum Customer Frame Size (octets)	Latency increase with Receive Diversity enabled (µs)
64	53
1500	64
9600	150

In all cases, the minimum latency does not change hence jitter is increased.

Link Planning for Spatial Diversity

Spatial Diversity can significantly improve the availability of a link, particularly for long links. Indeed regulations can recommend or even mandate that Spatial Diversity is deployed for links which are longer than a specific range.

LINKPlanner calculates link availability for all link configurations and provides a very convenient way of seeing the effect of enabling Spatial Diversity.

NOTE
When ACM is enabled, Spatial Diversity only increases the availability of the lowest configured modulation mode. The availability of higher order modes is not increased.

Planning 2+0 links

When planning 2+0 links, follow the process described in this section.

Concept of a 2+0 link

A 2+0 link consists of two independent 1+0 links which connect the same two sites and which share an antenna. The two 1+0 links must operate on different frequencies and so a separate license is generally required for each 1+0 link. The two 1+0 links are managed independently as two separate links.

NOTE

Link aggregation can be achieved by deployment of a suitable Ethernet switch at each end of the link. This is outside the scope of this user guide.

Antenna, RFU and CMU configurations for 2+0

CAUTION

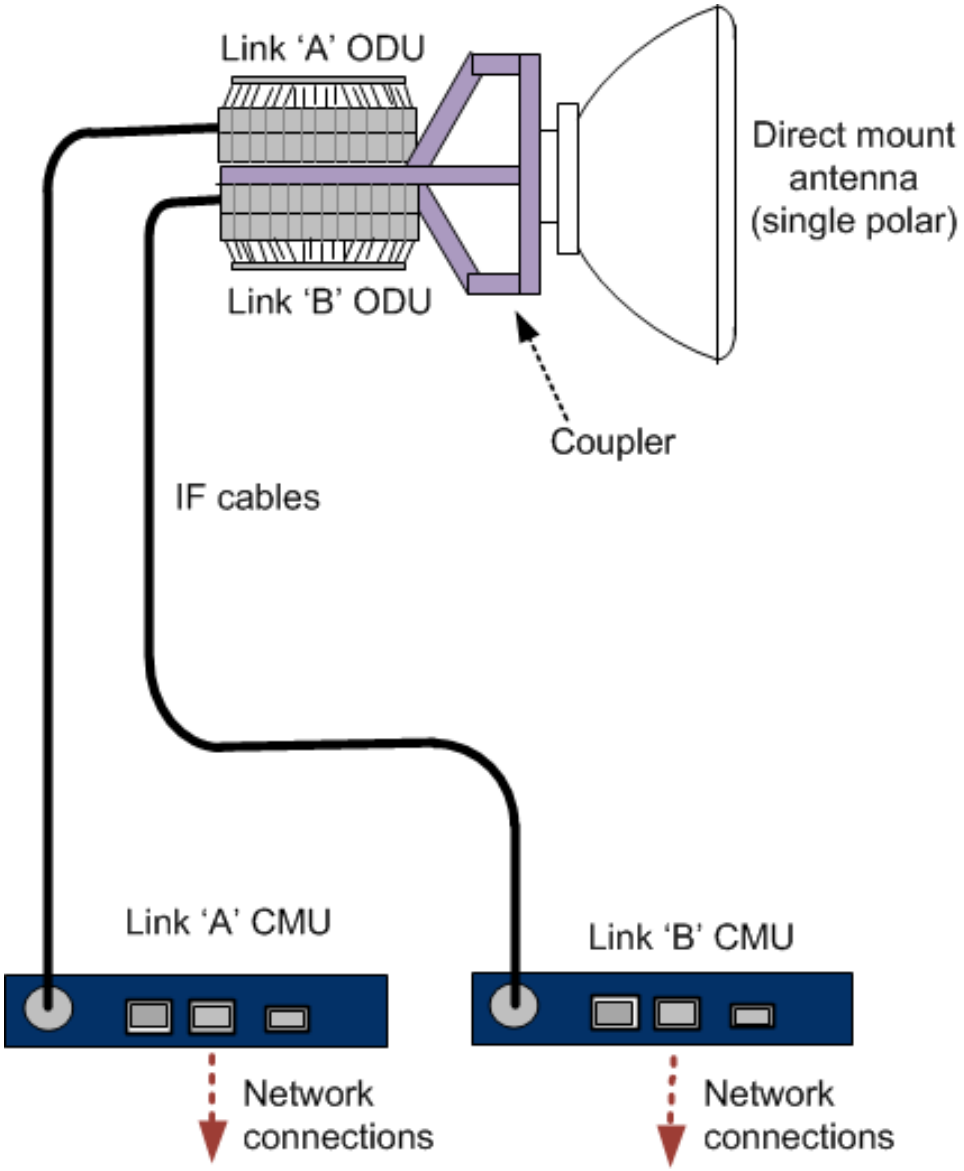
Do not install an ODU and an IRFU in the same link, as they cannot interwork.

Select one of the following 2+0 link end configurations:

ODUs coupled to single direct mount antenna - co-polar links

The Coupler mounts directly to the back of the antenna (Figure 62). An equal coupler will normally be selected to give the two 1+0 links equal link budget.

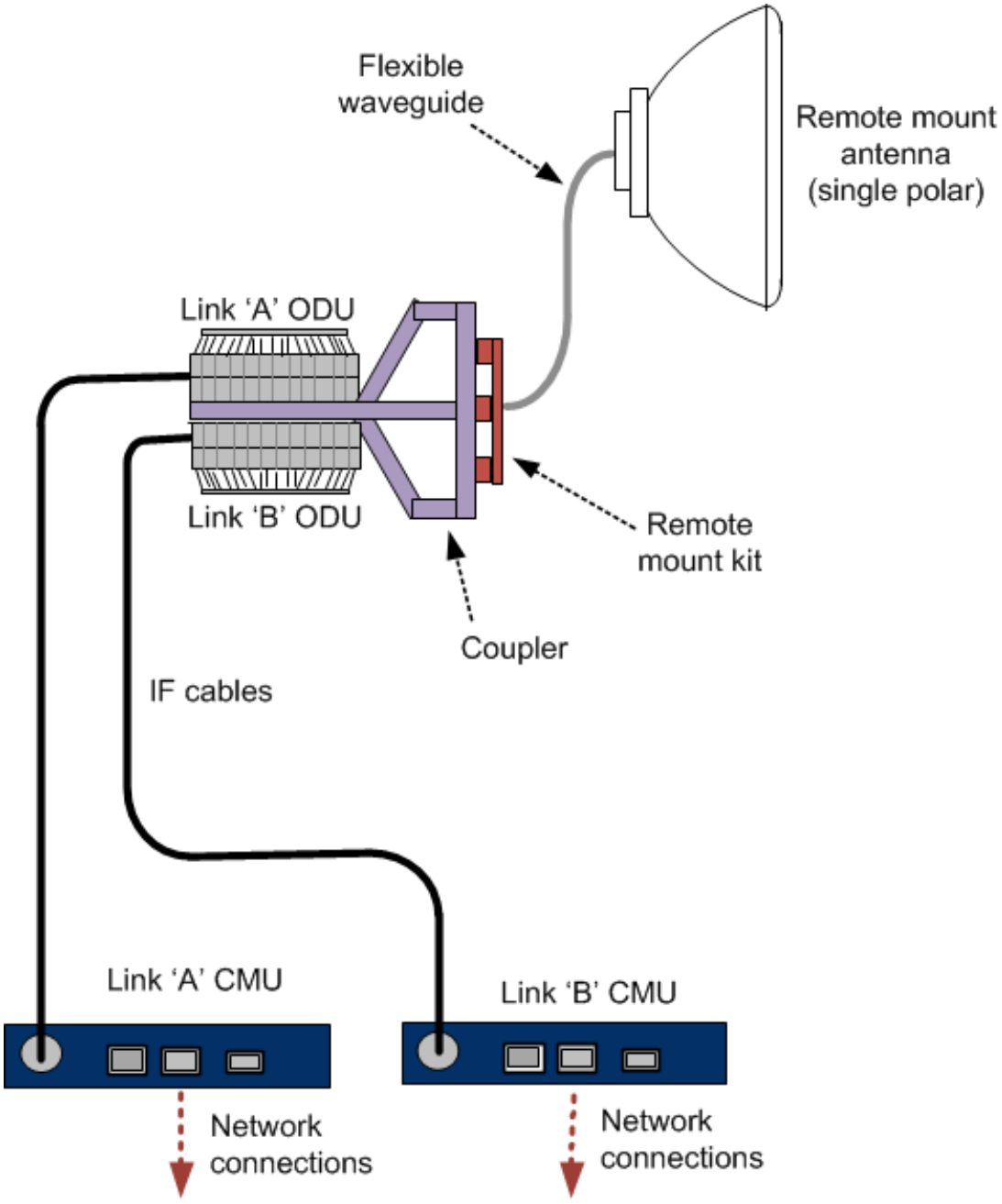
Figure 62 ODUs coupled to single direct mount antenna - co-polar links (schematic)



ODUs coupled to a single remote mount antenna - co-polar links

Requires a Remote Mount Kit (RMK) to mount the Coupler and 3' of flexible waveguide to connect the RMK to the antenna (Figure 63). An equal coupler will normally be selected to give the two 1+0 links equal link budget.

Figure 63 ODUs coupled to a single remote mount antenna - co-polar links (schematic)

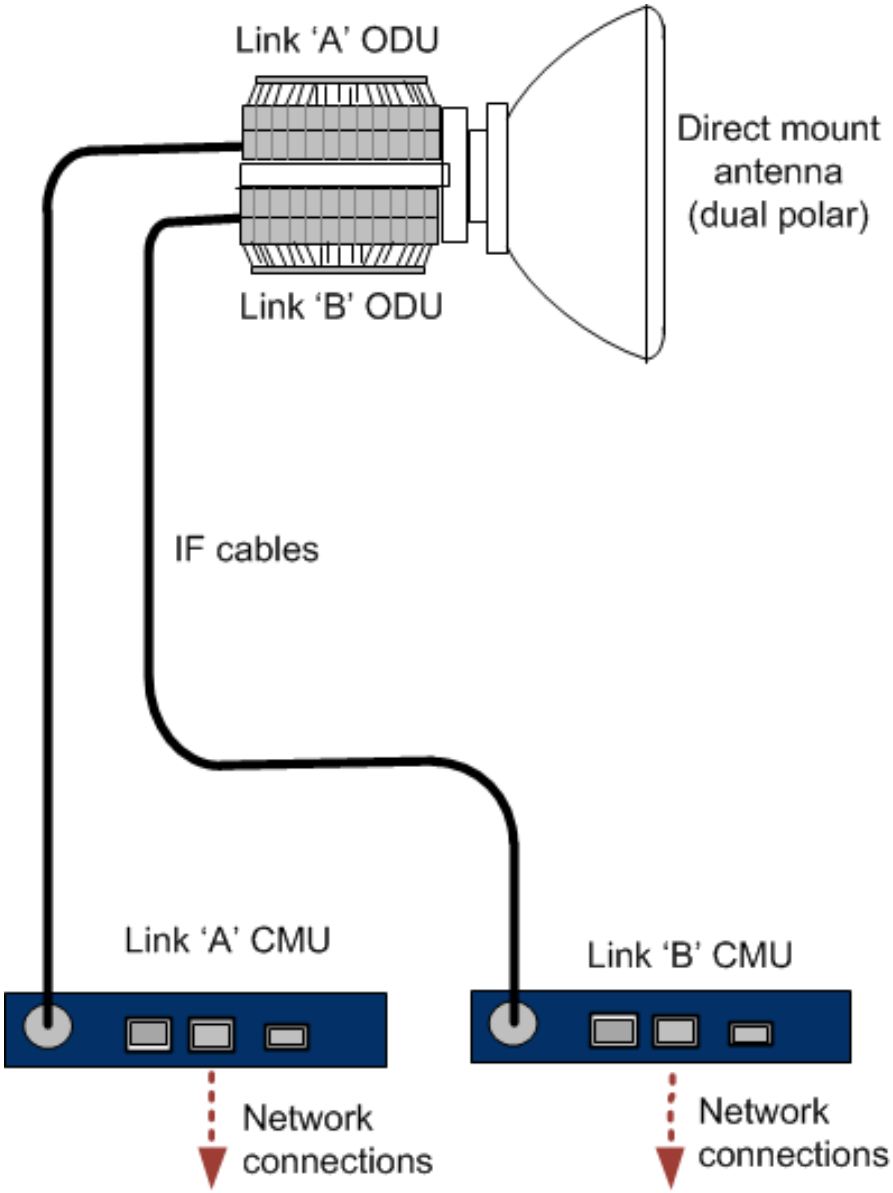


ODUs coupled to a single direct mount antenna - cross-polar links

Requires a direct mount dual polar antenna (Figure 64).

> **NOTE**
> To upgrade any standard antenna to a direct mount dual polar antenna, purchasing an orthogonal mount kit from Cambium.

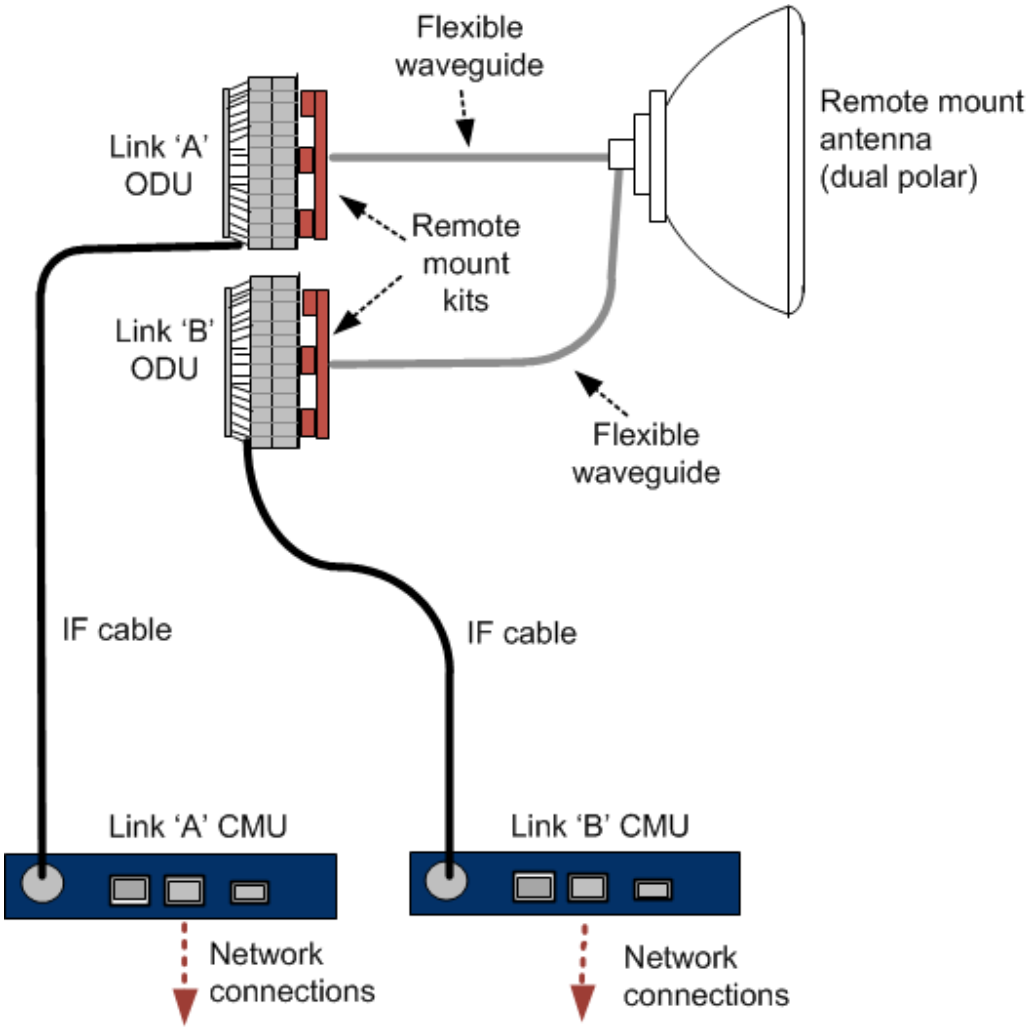
Figure 64 ODUs coupled to a single direct mount antenna - cross-polar links (schematic)



ODUs connected to a dual polar remote mount antenna - cross-polar links

Requires two Remote Mount Kits (RMK) to mount the ODUs and two 3' flexible waveguide to connect the RMKs to the antenna (Figure 65).

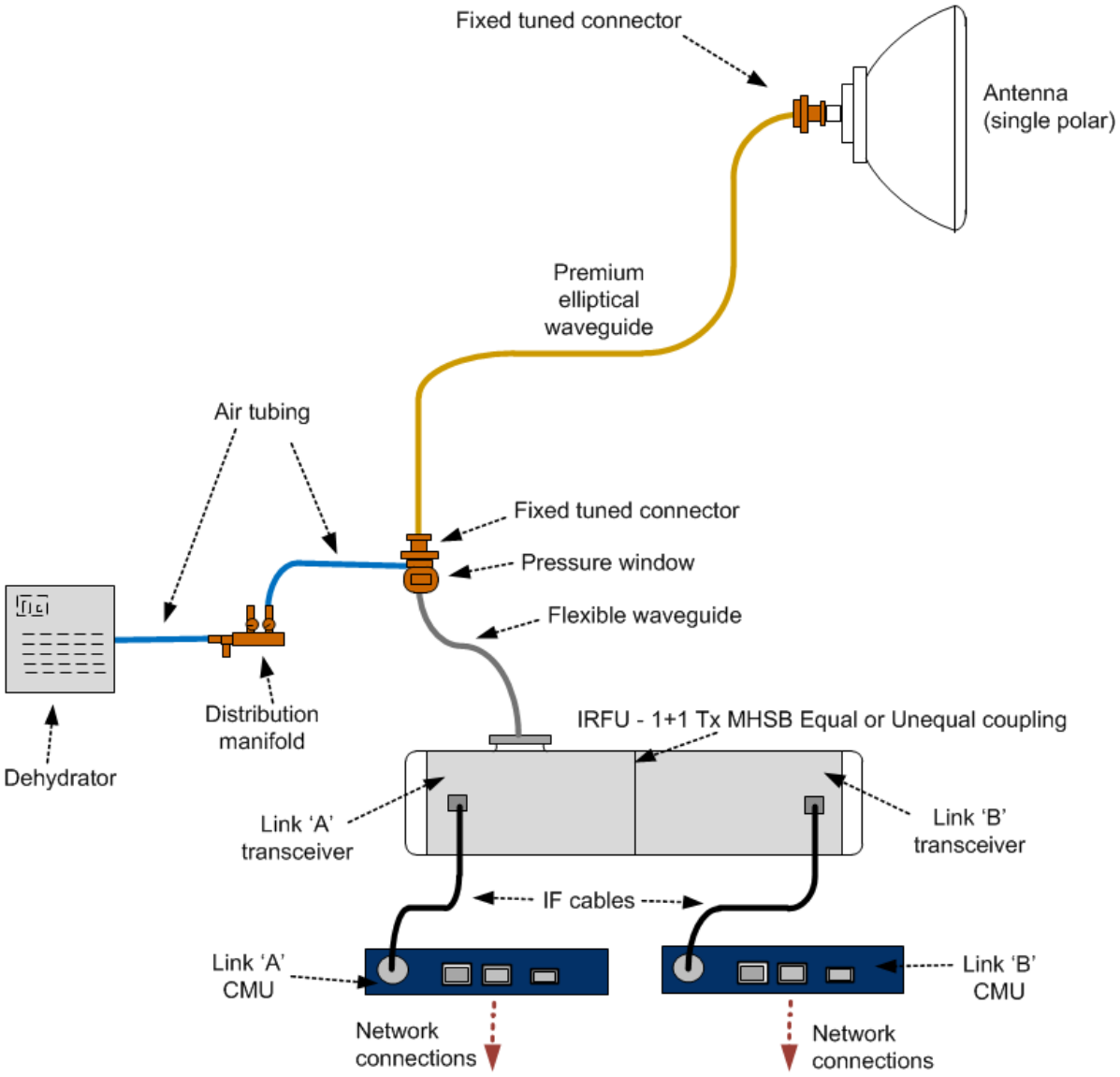
Figure 65 ODUs connected to a dual polar remote mount antenna - cross-polar links (schematic)



IRFU 2+0 with single remote mount antenna

Requires a length of elliptical waveguide dependant on the distance between the antenna and the IRFU (Figure 66). Requires waveguide dehydration accessories. The receiver coupling is internal to the IRFU. The IRFU may be purchased with equal or unequal coupling, the unequal coupling option provides a better link budget (nominally 6 dB) for the Primary transceivers.

Figure 66 IRFU 2+0 with single remote mount antenna (schematic)



Network configurations for 2+0

In a 2+0 configuration, Link ‘A’ and Link ‘B’ are independent. Each CMU is connected to the network using one of the methods described in Network configurations for 1+0 on page 2-34. The two links may be managed in different ways, for example Link ‘A’ may be out-of-band and Link ‘B’ may be in-band.

Frequency spacing in 2+0 ODU based links

For co-polar deployments, the transmit frequency of link A and link B at a given end must be separated by at least two channel separations. For example, if the channel separation is configured as 28 MHz, the spacing between the two transmit frequencies must be at least 56 MHz.

For cross-polar deployments, the transmit frequency of link A and link B at a given end must be separated by at least one channel separation. For example, if the channel separation is configured as 28 MHz, the spacing between the two transmit frequencies must be at least 28 MHz.

Frequency spacing in 2+0 IRFU based links

In a 2+0 IRFU-based link, plan the four transmit frequencies to meet the following requirements:

- At each link end, the two transmit frequencies must be separated by at least the amount quoted in Table 13.
- At each link end, the transmit and receive frequencies must be separated by at least the amount quoted in Table 14.

Table 13 Minimum transmit/transmit frequency separation at a 2+0 IRFU link end

Channel bandwidth	Band	RF filter bandwidth	Minimum separation between transmit frequencies
25, 30, 40 MHz	6 GHz, 11 GHz	30 MHz	70 MHz
		40 MHz	80 MHz
10 MHz	6 GHz	30 MHz	40 MHz
10 MHz	11 GHz	30 MHz	60 MHz
		40 MHz	70 MHz

Table 14 Minimum transmit/receive frequency separation at a 2+0 IRFU link end

Band	RF filter bandwidth	Minimum separation between transmit and receive frequencies (*)
6 GHz	30 MHz	70 MHz
11 GHz	30 MHz	80 MHz
	40 MHz	100 MHz

(*) This is the minimum allowed separation between the four combinations of transmit/receive frequency. For example, in the 6 GHz band with an RF filter bandwidth of 30 MHz:

- Link ‘A’ Tx and Link ‘A’ Rx must be separated by at least 70 MHz.
- Link ‘A’ Tx and Link ‘B’ Rx must be separated by at least 70 MHz.
- Link ‘B’ Tx and Link ‘A’ Rx must be separated by at least 70 MHz.
- Link ‘B’ Tx and Link ‘B’ Rx must be separated by at least 70 MHz.

Ordering components

This section describes how to select components for a planned PTP 800 link.

Ordering CMUs

Determine the number of compact modem units (CMUs) required per link, as follows:

- 1+0 links: 2 CMUs.
- 1+1 Hot Standby links: 4 CMUs.
- 2+0 links: 4 CMUs.

Order CMU kits from Cambium:

> ‘PTP800 Modem 1000/100BaseT with Capacity CAP 10 Mbps’,
> Cambium part number: WB3480.

Kit contents: one CMU, CMU bracket, power connector, ground lug.

Select optional CMU components from Table 15.

Table 15 Optional components for PTP 800 CMUs

Item	Cambium description, part number and notes
AC to DC power supply convertor 	Output voltage -48 VDC. No mains cable included. ‘AC-DC Power Supply Convertor’. Cambium part number WB3622.
DC connector	A DC connector is supplied in the CMU kit. Compatible DC connectors are also available from three manufacturers: Molex: 395305004 Tyco: 4-796634-4 Phoenix Contact: 1757035

Item	Cambium description, part number and notes
Mains Lead (for AC to DC converter)	'Mains Lead- US 3pin to C5 (PTP800 AC-DC PSU)'. Cambium part number WB3618. 'Mains Lead- UK 3pin to C5 (PTP800 AC-DC PSU)'. Cambium part number WB3619. 'Mains Lead- EU with dual earth to C5 (PTP800 AC-DC PSU)'. Cambium part number WB3620. 'Mains Lead- AUS 3pin to C5 (PTP800 AC-DC PSU)'. Cambium part number WB3621. **⚠ CAUTION** Use only appropriately rated and approved mains leads, in accordance with the regulations of the country of use.
CMU rack mounting kit 	Required for rack-mounted CMUs. 'PTP800 CMU/PTP-SYNC 19inch Rack Mount Installation Kit'. Cambium part number WB3486. Kit contents: bracket, washers, screws, nuts, handles and rack mount blank plate.
Right angle IF cable connector	A right angle connector can make it easier to install the CMU in the rack. 'RF CONNECTOR,N,MALE,RIGHT ANGLE FOR CNT-400 CABLE'. Cambium part number 01010589001.

Ordering antennas

> **NOTE**
> Applies to ODU deployments only.

Use Table 16 to select the type and quantity of antennas required per link.

Table 16 Selecting antennas for each hardware configuration

Hardware configuration	Antenna mounting	Antenna protection?	Antenna polarization	Quantity per link
1+0	Direct or remote (*1)	-	Single	2
1+1	Direct or remote	No	Single	2
1+1	Direct or remote	Yes	Single	4
2+0 co-polar	Direct or remote	-	Single	2
2+0 cross-polar	Direct or remote (*2)	-	Dual	2

(*1) Select single-polar antennas (direct or remote mount) for normal 1+0 links. Alternatively, to provide for a future upgrade from 1+0 to 2+0, select dual-polar remote mount antennas.

(*2) As an alternative to purchasing a dual-polar direct mount antenna, use an orthogonal mount kit (OMK) to upgrade any standard antenna to dual-polar direct mount; refer to Ordering OMKs on page 2-90.

> **NOTE**
> Only low VSWR antennas are supported for IRFU based installations. Use PTP LINKPlanner to confirm that the selected antenna is compatible with the IRFU.

Select antennas from the following tables:

- Lower 6 GHz and Upper 6 GHz: Table 17 and Table 18.
- 7 GHz and 8 GHz: Table 19 and Table 20.
- 11 GHz: Table 21 and Table 22.
- 13 GHz: Table 23 and Table 24.
- 15 GHz: Table 25 and Table 26.
- 18 GHz: Table 27 and Table 28.
- 23 GHz: Table 29 and Table 30.
- 26 GHz: Table 31 and Table 32.
- 28 GHz: Table 33 and Table 34.

- 32 GHz: Table 35 and Table 36.
- 38 GHz: Table 37 and Table 38.
- Parabolic radomes (optional): Table 39.

In the Interface column of these tables, ‘Direct’ means Cambium direct mount and a flange size, for example ‘PDR70’, means remote mount.

Table 17 Antennas: 6 GHz single polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beamwidth	Weight
85009298001	1.0 m (3 ft)	Direct	33 dBi	3.3°	24 kg (53 lb)
85010089050	1.2 m (4 ft)	Direct	35 dBi	2.9°	55 kg (121 lb)
85010089021	1.8 m (6 ft)	Direct	39 dBi	1.8°	62 kg (137 lb)
85010091022	1.0 m (3 ft)	PDR70	33 dBi	3.3°	24 kg (53 lb)
85010091024	1.2 m (4 ft)	PDR70	35 dBi	2.9°	55 kg (121 lb)
85010091007	1.8 m (6 ft)	PDR70	39 dBi	1.8°	62 kg (137 lb)
85009294001	1.8 m (6 ft)	CPR137G	38.2 dBi	1.9°	78 kg (172 lb)
85009294002	2.4 m (8 ft)	CPR137G	40.8 dBi	1.4°	114 kg (251 lb)
85009294003	3 m (10 ft)	CPR137G	43.4 dBi	1.1°	144 kg (317 lb)
85009294004	3.7 m (12 ft)	CPR137G	44.9 dBi	0.9°	245 kg (540 lb)

Table 18 Antennas: 6 GHz dual polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beamwidth	Weight
85009302001	1.0 m (3 ft)	Direct (*)	33 dBi	3.3°	
85009302002	1.2 m (4 ft)	Direct (*)	35 dBi	2.9°	
85009302003	1.8 m (6 ft)	Direct (*)	39 dBi	1.8°	
85010092048	1.0 m (3 ft)	PDR70	33 dBi	3.3°	24 kg (53 lb)
85010092060	1.2 m (4 ft)	PDR70	35 dBi	2.9°	55 kg (121 lb)
85010092021	1.8 m (6 ft)	PDR70	39 dBi	1.8°	62 kg (137 lb)

(*) The antenna includes an orthogonal mode transducer.

Table 19 Antennas: 7 GHz and 8 GHz single polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beamwidth	Weight
85010089045	0.6 m (2 ft)	Direct	31.1 dBi	4.7°	11 kg (25 lb)
85009298002	1.0 m (3 ft)	Direct	35.5 dBi	2.6°	24 kg (53 ib)
85010089051	1.2 m (4 ft)	Direct	37.3 dBi	2.2°	55 kg (121 lb)
85010089025	1.8 m (6 ft)	Direct	40.8 dBi	1.5°	62 kg (137 lb)
85010091020	0.6 m (2 ft)	PDR84	31.1 dBi	4.7°	11 kg (25 lb)
85010091023	1.0 m (3 ft)	PDR84	35.5 dBi	2.6°	24 kg (53 lb)
85010091025	1.2 m (4 ft)	PDR84	37.3 dBi	2.2°	55 kg (121 lb)
85010091011	1.8 m (6 ft)	PDR84	40.8 dBi	1.5°	62 kg (137 lb)

Table 20 Antennas: 7 GHz and 8 GHz dual polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beamwidth	Weight
85009303001	0.6 m (2 ft)	Direct (*)	31.1 dBi	4.7°	
85009303002	1.0 m (3 ft)	Direct (*)	35.5 dBi	2.6°	
85009303003	1.2 m (4 ft)	Direct (*)	37.3 dBi	2.2°	
85009303004	1.8 m (6 ft)	Direct (*)	40.6 dBi	1.5 °	
85010092051	0.6 m (2 ft)	PDR84	31.1 dBi	4.7°	14 kg (31 lb)
85010092059	1.0 m (3 ft)	PDR84	35.5 dBi	2.6°	24 kg (53 lb)
85010092061	1.2 m (4 ft)	PDR84	37.3 dBi	2.2°	55 kg (121 lb)
85010092025	1.8 m (6 ft)	PDR84	40.6 dBi	1.5 °	62 kg (137 lb)

(*) The antenna includes an orthogonal mode transducer.

Table 21 Antennas: 11 GHz single polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beamwidth	Weight
85010089049	0.6 m (2 ft)	Direct	34.5 dBi	3.3°	11 kg (25 lb)
85010089003	0.8 m (2.6 ft)	Direct	37.4 dBi	2.1°	30 kg (66 lb)
85009298003	1.0 m (3 ft)	Direct	38.4 dBi	2.0°	24 kg (53 lb)
85010089052	1.2 m (4 ft)	Direct	40.4 dBi	1.5°	46 kg (101 lb)
85010089005	1.8 m (6 ft)	Direct	43.8 dBi	1.1°	84 kg (185 lb)
85010091019	0.6 m (2 ft)	PDR100 (*1)	34.5 dBi	3.3°	11 kg (25 lb)
85010091003	0.8 m (2.6 ft)	PDR100 (*1)	37.4 dBi	2.1°	30 kg (66 lb)
85010091017	1.0 m (3 ft)	PDR100 (*1)	38.4 dBi	2.0°	24 kg (53 lb)
85010091026	1.2 m (4 ft)	PDR100 (*1)	40.4 dBi	1.5°	46 kg (101 lb)
85010091005	1.8 m (6 ft)	PDR100 (*1)	43.8 dBi	1.1°	84 kg (185 lb)

(*1) Waveguide interface 11 GHz antennas require a tapered transition (Table 58).

Table 22 Antennas: 11 GHz dual polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beamwidth	Weight
85009304001	0.6 m (2 ft)	Direct (*1)	34.5 dBi	3.3°	
85009304002	1.0 m (3 ft)	Direct (*1)	38.4 dBi	2.0°	
85009304003	1.2 m (4 ft)	Direct (*1)	40.4 dBi	1.5°	
85009304004	1.8 m (6 ft)	Direct (*1)	43.8 dBi	1.1°	
85010092052	0.6 m (2 ft)	PDR100 (*2)	34.5 dBi	3.3°	11 kg (25 lb)
85010092003	0.8 m (2.6 ft)	PDR100 (*2)	37.2 dBi	2.1°	30 kg (66 lb)
85010092042	1.0 m (3 ft)	PDR100 (*2)	38.4 dBi	2.0°	24 kg (53 lb)
85010092062	1.2 m (4 ft)	PDR100 (*2)	40.4 dBi	1.5°	46 kg (101 lb)
85010092005	1.8 m (6 ft)	PDR100 (*2)	43.8 dBi	1.1°	84 kg (185 lb)

(*1) The antenna includes an orthogonal mode transducer.

(*2) Waveguide interface 11 GHz antennas require a tapered transition (Table 58).

NOTE
The 11 GHz waveguide interface antennas require an extra component, the 11 GHz tapered transition. This is supplied by Cambium (Table 58) and is required to convert between the antenna interface and the waveguide flange.

Table 23 Antennas: 13 GHz single polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beamwidth	Weight
85010089053	0.3 m (1 ft)	Direct	30.9 dBi	4.7°	7 kg (15 lb)
85010089046	0.6 m (2 ft)	Direct	36.0 dBi	2.7°	11 kg (25 lb)
85009298004	1.0 m (3 ft)	Direct	40.0 dBi	1.6°	24 kg (53 lb)
85010089054	1.2 m (4 ft)	Direct	42.0 dBi	1.3°	55 kg (121 lb)
85010089030	1.8 m (6 ft)	Direct	45.2 dBi	0.9°	62 kg (137 lb)
85010091012	0.3 m (1 ft)	PBR120	30.9 dBi	4.7°	7 kg (15 lb)
85010091021	0.6 m (2 ft)	PBR120	36.0 dBi	2.7°	11 kg (25 lb)
85010091018	1.0 m (3 ft)	PBR120	40.0 dBi	1.6°	24 kg (53 lb)
85010091027	1.2 m (4 ft)	PBR120	42.0 dBi	1.3°	55 kg (121 lb)
85010091016	1.8 m (6 ft)	PBR120	45.2 dBi	0.9°	62 kg (137 lb)

Table 24 Antennas: 13 GHz dual polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beamwidth	Weight
85009305001	0.3 m (1 ft)	Direct (*)	30.9 dBi	4.7°	
85009305002	0.6 m (2 ft)	Direct (*)	36.0 dBi	2.7°	
85009305003	1.0 m (3 ft)	Direct (*)	40.0 dBi	1.6°	
85009305004	1.2 m (4 ft)	Direct (*)	42.0 dBi	1.3°	
85009305005	1.8 m (6 ft)	Direct (*)	45.2 dBi	0.9°	
85010092026	0.3 m (1 ft)	PBR120	30.9 dBi	4.7°	7 kg (15 lb)
85010092056	0.6 m (2 ft)	PBR120	36.0 dBi	2.7°	11 kg (25 lb)
85010092043	1.0 m (3 ft)	PBR120	40.0 dBi	1.6°	24 kg (53 lb)
85010092063	1.2 m (4 ft)	PBR120	42.0 dBi	1.3°	55 kg (121 lb)
85010092030	1.8 m (6 ft)	PBR120	45.2 dBi	0.9°	62 kg (137 lb)

(*) The antenna includes an orthogonal mode transducer.

Table 25 Antennas: 15 GHz single polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beamwidth	Weight
85010089055	0.3 m (1 ft)	Direct	32.1 dBi	4.3°	7 kg (15 lb)
85010089047	0.6 m (2 ft)	Direct	36.8 dBi	2.5 °	11 kg (25 lb)
85009298005	1.0 m (3 ft)	Direct	41.1 dBi	1.5°	24 kg (53 lb)
85010089056	1.2 m (4 ft)	Direct	42.9 dBi	1.2°	55 kg (121 lb)
85010089035	1.8 m (6 ft)	Direct	46.2 dBi	0.8°	62 kg (137 lb)

Table 26 Antennas: 15 GHz dual polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beamwidth	Weight
85009306001	0.3 m (1 ft)	Direct (*)	32.0 dBi	4.3°	
85009306002	0.6 m (2 ft)	Direct (*)	36.8 dBi	2.5°	
85009306003	1.0 m (3 ft)	Direct (*)	41.1 dBi	1.5°	
85009306004	1.2 m (4 ft)	Direct (*)	42.9 dBi	1.2°	
85009306005	1.8 m (6 ft)	Direct (*)	46.2 dBi	0.8°	
85010092031	0.3 m (1 ft)	PBR140	32.0 dBi	4.3°	7 kg (15 lb)
85010092057	0.6 m (2 ft)	PBR140	36.8 dBi	2.5°	11 kg (25 lb)
85010092044	1.0 m (3 ft)	PBR140	41.1 dBi	1.5°	24 kg (53 lb)
85010092064	1.2 m (4 ft)	PBR140	42.9 dBi	1.2°	55 kg (121 lb)
85010092035	1.8 m (6 ft)	PBR140	46.2 dBi	0.8°	62 kg (137 lb)

(*) The antenna includes an orthogonal mode transducer.

Table 27 Antennas: 18 GHz single polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beamwidth	Weight
85010089057	0.3 m (1 ft)	Direct	34.2 dBi	3.3°	6 kg (13 lb)
85010089042	0.6 m (2 ft)	Direct	38.9 dBi	2.1°	11 kg (25 lb)
85009298006	1.0 m (3 ft)	Direct	43.5 dBi	1.1°	24 kg (53 lb)
85010089058	1.2 m (4 ft)	Direct	44.7 dBi	0.9°	46 kg (101 lb)
85010089010	1.8 m (6 ft)	Direct	47.8 dBi	0.7°	84 kg (185 lb)

Table 28 Antennas: 18 GHz dual polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beamwidth	Weight
85009307001	0.3 m (1 ft)	Direct (*)	34.2 dBi	3.3°	
85009307002	0.6 m (2 ft)	Direct (*)	38.9 dBi	2.1°	
85009307003	1.0 m (3 ft)	Direct (*)	43.5 dBi	1.1°	
85009307004	1.2 m (4 ft)	Direct (*)	44.7 dBi	0.9°	
85009307005	1.8 m (6 ft)	Direct (*)	47.6 dBi	0.7°	
85010092006	0.3 m (1 ft)	PBR220	34.2 dBi	3.3°	6 kg (13 lb)
85010092053	0.6 m (2 ft)	PBR220	38.9 dBi	2.1°	11 kg (25 lb)
85010092045	1.0 m (3 ft)	PBR220	43.5 dBi	1.1°	24 kg (53 lb)
85010092065	1.2 m (4 ft)	PBR220	44.7 dBi	0.9°	46 kg (101 lb)
85010092010	1.8 m (6 ft)	PBR220	47.6 dBi	0.7°	84 kg (185 lb)

(*) The antenna includes an orthogonal mode transducer.

Table 29 Antennas: 23 GHz single polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beam-width	Weight
85010089059	0.3 m (1 ft)	Direct	35.3 dBi	3.0°	6 kg (13 lb)
85010089043	0.6 m (2 ft)	Direct	40.5 dBi	1.7°	11 kg (25 lb)
85009298007	1.0 m (3 ft)	Direct	44.8 dBi	1.0°	24 kg (53 lb)
85010089060	1.2 m (4 ft)	Direct	46.7 dBi	0.8°	46 kg (101 lb)
85010089015	1.8 m (6 ft)	Direct	49.4 dBi	0.5°	84 kg (185 lb)

Table 30 Antennas: 23 GHz dual polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beam-width	Weight
85009308001	0.3 m (1 ft)	Direct (*)	35.3 dBi	3.0°	
85009308002	0.6 m (2 ft)	Direct (*)	40.5 dBi	1.7°	
85009308003	1.0 m (3 ft)	Direct (*)	44.8 dBi	1.0°	
85009308004	1.2 m (4 ft)	Direct (*)	46.7 dBi	0.8°	
85009308005	1.8 m (6 ft)	Direct (*)	49.2 dBi	0.5°	
85010092011	0.3 m (1 ft)	PBR220	35.3 dBi	3.0°	6 kg (13 lb)
85010092054	0.6 m (2 ft)	PBR220	40.5 dBi	1.7°	11 kg (25 lb)
85010092046	1.0 m (3 ft)	PBR220	44.8 dBi	1.0°	24 kg (53 lb)
85010092066	1.2 m (4 ft)	PBR220	46.7 dBi	0.8°	46 kg (101 lb)
85010092015	1.8 m (6 ft)	PBR220	49.2 dBi	0.5°	84 kg (185 lb)

(*) The antenna includes an orthogonal mode transducer.

Table 31 Antennas: 26 GHz single polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beam-width	Weight
85010089061	0.3 m (1 ft)	Direct	36.6 dBi	2.5°	6 kg (13 lb)
85010089044	0.6 m (2 ft)	Direct	41.6 dBi	1.5°	11 kg (25 lb)
85009298008	1.0 m (3 ft)	Direct	45.8 dBi	0.8°	24 kg (53 lb)
85010089062	1.2 m (4 ft)	Direct	47.4 dBi	0.6°	46 kg (101 lb)

Table 32 Antennas: 26 GHz dual polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beam-width	Weight
85010092016	0.3 m (1 ft)	PBR220	36.6 dBi	2.5°	6 kg (13 lb)
85010092055	0.6 m (2 ft)	PBR220	41.6 dBi	1.5°	11 kg (25 lb)
85010092047	1.0 m (3 ft)	PBR220	45.8 dBi	0.8°	24 kg (53 lb)
85010092067	1.2 m (4 ft)	PBR220	47.4 dBi	0.6°	46 kg (101 lb)

Table 33 Antennas: 28 GHz single polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beam-width	Weight
85010089064	0.3 m (1 ft)	Direct	38.1 dBi	2.2°	7 kg (14 lb)
85010089041	0.6 m (2 ft)	Direct	42.6 dBi	1.2°	11 kg (25 lb)

Table 34 Antennas: 28 GHz dual polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beam-width	Weight
85010092040	0.3 m (1 ft)	PBR320	38.1 dBi	2.2°	7 kg (14 lb)
85010092041	0.6 m (2 ft)	PBR320	42.6 dBi	1.2°	11 kg (25 lb)

Table 35 Antennas: 32 GHz single polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beam-width	Weight
85010089036	0.3 m (1 ft)	Direct	38.9 dBi	1.8°	7 kg (14 lb)
85010089037	0.6 m (2 ft)	Direct	43.5 dBi	1.0°	11 kg (25 lb)

Table 36 Antennas: 32 GHz dual polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beam-width	Weight
85010092036	0.3 m (1 ft)	PBR320	38.9 dBi	1.8°	7 kg (14 lb)
85010092037	0.6 m (2 ft)	PBR320	43.5 dBi	1.0°	11 kg (25 lb)

Table 37 Antennas: 38 GHz single polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beam-width	Weight
85010089063	0.3 m (1 ft)	Direct	40.1 dBi	1.6°	6 kg (13 lb)
85010089048	0.6 m (2 ft)	Direct	45.2 dBi	0.9°	11 kg (25 lb)

Table 38 Antennas: 38 GHz dual polarization

Cambium number	Diameter	Interface	Mid-band gain	Vertical beam-width	Weight
85010092038	0.3 m (1 ft)	PBR320	40.1 dBi	1.6°	7 kg (15 lb)
85010092058	0.6 m (2 ft)	PBR320	45.2 dBi	0.9°	11 kg (25 lb)

Table 39 Parabolic radomes (optional)

Cambium number	Description
85009295001	10 Foot Radome For Par10 Antenna
85009295002	11 Foot Radome For Par12 Antenna

Ordering ODUs

> **NOTE**
> Applies to ODU deployments only.

Determine the number of ODUs required per link, as follows:

- 1+0 links: 2 ODUs.
- 1+1 Hot Standby links: 4 ODUs.
- 2+0 links: 4 ODUs.

A link consists of one ODU operating in the low sub-band paired with another ODU operating in the high sub-band. For example in Table 40, 01010411007 (B1-Lo) is paired with 01010411008 (B1-Hi):

- 01010411007 transmits on a low sub-band frequency (for example 5925 MHz) and receives on a high sub-band frequency (for example 6175 MHz).
- 01010411008 transmits on a high sub-band frequency (for example 6175 MHz) and receives on a low sub-band frequency (for example 5925 MHz).

The T/R spacing column indicates the difference between Tx and Rx frequencies.

Select ODUs from the following tables:

- Lower 6 GHz: Table 40.
- Upper 6 GHz: Table 41.
- 7 GHz: Table 42.
- 8 GHz: Table 43.
- 11 GHz: Table 44 (ODU-B) and Table 45 (ODU-A).
- 13 GHz: Table 46.
- 15 GHz: Table 47.
- 18 GHz: Table 48 (ODU-B) and Table 49 (ODU-A).
- 23 GHz: Table 50 (ODU-B) and Table 51 (ODU-A).
- 26 GHz: Table 52.
- 28 GHz: Table 53.

- 32 GHz: Table 54.
- 38 GHz: Table 55.

> **NOTE**
> If ODU-B is available (11, 18 and 23 GHz), choose it in preference to ODU-A. Do not install ODU-A and ODU-B in the same link.

Table 40 ODUs: Lower 6 GHz ODU-A

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010411007	FCC, ETSI	B1-Lo	5925 – 6025 MHz	252 MHz
01010411008		B1-Hi	6175 – 6275 MHz	
01010411009		B2-Lo	6000 – 6100 MHz	
01010411010		B2-Hi	6250 – 6350 MHz	
01010411011		B3-Lo	6075 – 6175 MHz	
01010411012		B3-Hi	6325 – 6425 MHz	

Table 41 ODUs: Upper 6 GHz ODU-A

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010411024	FCC	B1-Lo	6580 – 6640 MHz	160 MHz
01010411022		B1-Hi	6740 – 6800 MHz	
01010411025		B2-Lo	6640 – 6710 MHz	
01010411023		B2-Hi	6800 – 6870 MHz	
01010411027	FCC	B1-Lo	6530 – 6580 MHz	170 MHz
01010411026		B1-Hi	6700 – 6750 MHz	
01010411013	ETSI	B1-Lo	6430 – 6540 MHz	340 MHz
01010411014		B1-Hi	6770 – 6880 MHz	
01010411015		B2-Lo	6520 – 6630 MHz	
01010411016		B2-Hi	6860 – 6970 MHz	
01010411017		B3-Lo	6600 – 6710 MHz	
01010411018		B3-Hi	6940 – 7050 MHz	
01010411019		B4-Lo	6670 – 6780 MHz	
01010411020		B4-Hi	7010 – 7120 MHz	

Table 42 ODUs: 7 GHz ODU-A

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010610001	ETSI	B1-Lo	7428 – 7484 MHz	154 MHz
01010610002		B1-Hi	7582 – 7638 MHz	
01010610003		B2-Lo	7470 – 7526 MHz	
01010610004		B2-Hi	7624 – 7680 MHz	
01010610005		B3-Lo	7512 – 7568 MHz	
01010610006		B3-Hi	7666 – 7722 MHz	
01010610013	ETSI	B1-Lo	7114 – 7177 MHz	161 MHz
01010610014		B1-Hi	7275 – 7338 MHz	
01010610015		B2-Lo	7149 – 7212 MHz	
01010610016		B2-Hi	7310 – 7373 MHz	
01010610017		B3-Lo	7184 – 7247 MHz	
01010610018		B3-Hi	7345 – 7408 MHz	
01010610019		B4-Lo	7219 – 7282 MHz	
01010610020		B4-Hi	7380 – 7443 MHz	
01010610021		B5-Lo	7239 – 7302 MHz	
01010610022		B5-Hi	7400 – 7463 MHz	
01010610023		B6-Lo	7274 – 7337 MHz	
01010610024		B6-Hi	7435 – 7498 MHz	
01010610025		B7-Lo	7309 – 7372 MHz	
01010610026		B7-Hi	7470 – 7533 MHz	
01010610027		B8-Lo	7344 – 7407 MHz	
01010610028		B8-Hi	7505 – 7568 MHz	
01010610029		B9-Lo	7414 – 7477 MHz	
01010610030		B9-Hi	7575 – 7638 MHz	
01010610031		B10-Lo	7449 – 7512 MHz	
01010610032		B10-Hi	7610 – 7673 MHz	
01010610033		B21-Lo	7484 – 7547 MHz	

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010610034		B21-Hi	7645 – 7708 MHz	
01010610035		B22-Lo	7519 – 7582 MHz	
01010610036		B22-Hi	7680 – 7743 MHz	
01010610037		B23-Lo	7539 – 7602 MHz	
01010610038		B23-Hi	7700 – 7763 MHz	
01010610039		B24-Lo	7574 – 7637 MHz	
01010610040		B24-Hi	7735 – 7798 MHz	
01010610041		B25-Lo	7609 – 7672 MHz	
01010610042		B25-Hi	7770 – 7833 MHz	
01010610043		B26-Lo	7644 – 7707 MHz	
01010610044		B26-Hi	7805 – 7868 MHz	
01010610062	ETSI	B1-Lo	7443 – 7499 MHz	168 MHz
01010610063		B1-Hi	7611 – 7667 MHz	
01010610064		B2-Lo	7485 – 7541 MHz	
01010610065		B2-Hi	7653 – 7709 MHz	
01010610066		B3-Lo	7527 – 7583 MHz	
01010610067		B3-Hi	7695 – 7751 MHz	
01010610045	ETSI	B1-Lo	7093 – 7149 MHz	196 MHz
01010610046		B1-Hi	7289 – 7345 MHz	
01010610047		B2-Lo	7121 – 7177 MHz	
01010610048		B2-Hi	7317 – 7373 MHz	
01010610049		B3-Lo	7149 – 7205 MHz	
01010610050		B3-Hi	7345 – 7401 MHz	
01010610051		B4-Lo	7177 – 7233 MHz	
01010610052		B4-Hi	7373 – 7429 MHz	
01010610053		B5-Lo	7205 – 7261 MHz	
01010610054		B5-Hi	7401 – 7457 MHz	
01010610055	ETSI	B1-Lo	7400 – 7484 MHz	245 MHz
01010610056		B1-Hi	7645 – 7729 MHz	

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010610057		B2-Lo	7484 – 7568 MHz	
01010610058		B2-Hi	7729 – 7813 MHz	
01010610059		B3-Lo	7568 – 7652 MHz	
01010610060		B3-Hi	7813 – 7897 MHz	
01010610068	NTIA	B1-Lo	7090 – 7210 MHz	300 MHz
01010610069		B1-Hi	7390 – 7510 MHz	
01010610070		B2-Lo	7210 – 7330 MHz	
01010610071		B2-Hi	7510 – 7630 MHz	
01010610072		B3-Lo	7330 – 7450 MHz	
01010610073		B3-Hi	7630 – 7750 MHz	

Table 43 ODUs: 8 GHz ODU-A

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010611001	ETSI	B1-Lo	8279 – 8307 MHz	119 MHz and 126 MHz
01010611002		B1-Hi	8398 – 8426 MHz	
01010611003		B2-Lo	8293 – 8321 MHz	
01010611004		B2-Hi	8412 – 8440 MHz	
01010611005		B3-Lo	8307 – 8335 MHz	
01010611006		B3-Hi	8426 – 8454 MHz	
01010611007		B4-Lo	8321 – 8349 MHz	
01010611008		B4-Hi	8440 – 8468 MHz	
01010611009		B5-Lo	8335 – 8363 MHz	
01010611010		B5-Hi	8454 – 8482 MHz	
01010611011		B6-Lo	8349 – 8377 MHz	
01010611012		B6-Hi	8468 – 8496 MHz	
01010611019	ETSI	B1-Lo	8043 – 8113 MHz	208 MHz
01010611020		B1-Hi	8251 – 8321 MHz	
01010611021		B2-Lo	8099 – 8169 MHz	
01010611022		B2-Hi	8307 – 8377 MHz	

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010611023		B3-Lo	8155 – 8225 MHz	
01010611024		B3-Hi	8363 – 8433 MHz	
01010611025		B4-Lo	8211 – 8281 MHz	
01010611026		B4-Hi	8419 – 8489 MHz	
01010611027	ETSI	B1-Lo	7905 – 8024 MHz	266 MHz
01010611028		B1-Hi	8171 – 8290 MHz	
01010611029		B2-Lo	8017 – 8136 MHz	
01010611030		B2-Hi	8283 – 8402 MHz	
01010611031	ETSI	B2-Lo	7835 – 7971 MHz	311 MHz
01010611032		B2-Hi	8146 – 8282 MHz	
01010611033		B3-Lo	7717 – 7867 MHz	
01010611034		B3-Hi	8028 – 8178 MHz	
01010611036	NTIA	B1-Lo	7750 – 7870 MHz	360 MHz
01010611037		B1-Hi	8110 – 8230 MHz	
01010611038		B2-Lo	7870 – 7990 MHz	
01010611039		B2-Hi	8230 – 8350 MHz	
01010611040		B3-Lo	7990 – 8110 MHz	
01010611041		B3-Hi	8350 – 8470 MHz	

Table 44 ODUs: 11 GHz ODU-B

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
85009317001	FCC	B5-Lo	10700 – 10890 MHz	490 MHz and 500 MHz
85009317002		B5-Hi	11200 – 11390 MHz	
85009317003		B6-Lo	10855 – 11045 MHz	
85009317004		B6-Hi	11355 – 11545 MHz	
85009317005		B7-Lo	11010 – 11200 MHz	
85009317006		B7-Hi	11510 – 11700 MHz	

Table 45 ODUs: 11 GHz ODU-A

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010208001	FCC, ETSI	B5-Lo	10700 – 10890 MHz	490 MHz and 500 MHz
01010208002		B5-Hi	11200 – 11390 MHz	
01010208003		B6-Lo	10855 – 11045 MHz	
01010208004		B6-Hi	11355 – 11545 MHz	
01010208005		B7-Lo	11010 – 11200 MHz	
01010208006		B7-Hi	11510 – 11700 MHz	
01010208007	ETSI	B1-Lo	10675 – 10855 MHz	530 MHz
01010208008		B1-Hi	11205 – 11385 MHz	
01010208009		B2-Lo	10795 – 10975 MHz	
01010208010		B2-Hi	11325 – 11505 MHz	
01010208011		B3-Lo	10915 – 11135 MHz	
01010208012		B3-Hi	11455 – 11665 MHz	
01010208013		B4-Lo	11035 – 11215 MHz	
01010208014		B4-Hi	11565 – 11745 MHz	

Table 46 ODUs: 13 GHz ODU-A

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010583001	ETSI	B1-Lo	12751 – 12814 MHz	266 MHz
01010583002		B1-Hi	13017 – 13080 MHz	
01010583003		B2-Lo	12807 – 12870 MHz	
01010583004		B2-Hi	13073 – 13136 MHz	
01010583005		B3-Lo	12863 – 12926 MHz	
01010583006		B3-Hi	13129 – 13192 MHz	
01010583007		B4-Lo	12919 – 12982 MHz	
01010583008		B4-Hi	13185 – 13248 MHz	

Table 47 ODUs: 15 GHz ODU-A

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010584001	ETSI	B4-Lo	14501 – 14613 MHz	420 MHz
01010584002		B4-Hi	14921 – 15033 MHz	
01010584003		B5-Lo	14606 – 14725 MHz	
01010584004		B5-Hi	15026 – 15145 MHz	
01010584005		B6-Lo	14718 – 14837 MHz	
01010584006		B6-Hi	15138 – 15257 MHz	
01010584007		B7-Lo	14816 – 14928 MHz	
01010584008		B7-Hi	15236 – 15348 MHz	
01010584009	ETSI	B4-Lo	14403 – 14522 MHz	490 MHz
01010584010		B4-Hi	14893 – 15012 MHz	
01010584011		B5-Lo	14515 – 14634 MHz	
01010584012		B5-Hi	15005 – 15124 MHz	
01010584013		B6-Lo	14627 – 14746 MHz	
01010584014		B6-Hi	15117 – 15236 MHz	
01010584015		B7-Lo	14739 – 14858 MHz	
01010584016		B7-Hi	15229 – 15348 MHz	
01010584020	ETSI	B2-Lo	14500 – 14625 MHz	728 MHz
01010584021		B2-Hi	15228 – 15353 MHz	
01010584022	Mexico, Italy	B1-Lo	14627 – 14746 MHz	315 MHz
01010584023		B1-Hi	14942 – 15061 MHz	
01010584024		B2-Lo	14725 – 14844 MHz	
01010584025		B2-Hi	15040 – 15159 MHz	
01010584026		B3-Lo	14823 – 14942 MHz	
01010584027		B3-Hi	15138 – 15257 MHz	
01010584028	ETSI	B1-Lo	14400 – 14512 MHz	644 MHz
01010584029		B1-Hi	15044 – 15156 MHz	
01010584030		B2-Lo	14498 – 14610 MHz	
01010584031		B2-Hi	15142 – 15254 MHz	

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010584032		B3-Lo	14596 – 14708 MHz	
01010584033		B3-Hi	15240 – 15352 MHz	

Table 48 ODUs: 18 GHz ODU-B

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
85009318001	FCC	B3-Lo	17700 – 18140 MHz	1560 MHz
85009318002		B3-Hi	19260 – 19700 MHz	

Table 49 ODUs: 18 GHz ODU-A

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010209001	ETSI	B1-Lo	17685 – 17985 MHz	1010 MHz and 1008 MHz
01010209002		B1-Hi	18695 – 18995 MHz	
01010209003		B2-Lo	17930 – 18230 MHz	
01010209004		B2-Hi	18940 – 19240 MHz	
01010209005		B3-Lo	18180 – 18480 MHz	
01010209006		B3-Hi	19190 – 19490 MHz	
01010209007		B4-Lo	18400 – 18700 MHz	
01010209008		B4-Hi	19410 – 19710 MHz	
01010209013	FCC, Brazil	B3-Lo	17700 – 18140 MHz	1560 MHz
01010209014		B3-Hi	19260 – 19700 MHz	

Table 50 ODUs: 23 GHz ODU-B

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
85009319001	FCC	B5-Lo	21200 – 21600 MHz	1200 MHz
85009319002		B5-Hi	22400 – 22800 MHz	
85009319003		B6-Lo	21600 – 22000 MHz	
85009319004		B6-Hi	22800 – 23200 MHz	
85009319005		B7-Lo	22000 – 22400 MHz	
85009319006		B7-Hi	23200 – 23600 MHz	

Table 51 ODUs: 23 GHz ODU-A

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010210001	ETSI	B1-Lo	21994 – 22330 MHz	1008 MHz
01010210002		B1-Hi	23002 – 23338 MHz	
01010210003		B2-Lo	22274 – 22610 MHz	
01010210004		B2-Hi	23282 – 23618 MHz	
01010210005	FCC	B5-Lo	21200 – 21600 MHz	1200 MHz
01010210006		B5-Hi	22400 – 22800 MHz	
01010210007		B6-Lo	21600 – 22000 MHz	
01010210008		B6-Hi	22800 – 23200 MHz	
01010210009		B7-Lo	22000 – 22400 MHz	
01010210010		B7-Hi	23200 – 23600 MHz	
01010210011	ETSI	B1-Lo	21200 – 21500 MHz	1232 MHz
01010210012		B1-Hi	22432 – 22732 MHz	
01010210013		B2-Lo	21472 – 21786 MHz	
01010210014		B2-Hi	22704 – 23018 MHz	
01010210015		B3-Lo	21779 – 22093 MHz	
01010210016		B3-Hi	23011 – 23325 MHz	
01010210017		B4-Lo	22086 – 22386 MHz	

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010210018		B4-Hi	23318 – 23618 MHz	

Table 52 ODUs: 26 GHz ODU-A

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010403003	ETSI	B1-Lo	24549 – 24885 MHz	1008 MHz
01010403004		B1-Hi	25557 – 25893 MHz	
01010403005		B2-Lo	24829 – 25165 MHz	
01010403006		B2-Hi	25837 – 26173 MHz	
01010403007		B3-Lo	25109 – 25445 MHz	
01010403008		B3-Hi	26117 – 26453 MHz	
01010403001	FCC	B1-Lo	24250 – 24450 MHz	800 MHz
01010403002		B1-Hi	25050 – 25250 MHz	

Table 53 ODUs: 28 GHz ODU-A

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01009420001	ETSI	B1-Lo	27520 – 28025 MHz	1008 MHz
01009420002		B1-Hi	28528 – 29033 MHz	
01009420003		B2-Lo	27968 – 28473 MHz	
01009420004		B2-Hi	28976 – 29481 MHz	

Table 54 ODUs: 32 GHz ODU-A

Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010612001	ETSI	B1-Lo	31815 – 32207 MHz	812 MHz
01010612002		B1-Hi	32627 – 33019 MHz	
01010612003		B2-Lo	32179 – 32571 MHz	
01010612004		B2-Hi	32991 – 33383 MHz	

Table 55 ODUs: 38 GHz ODU-A

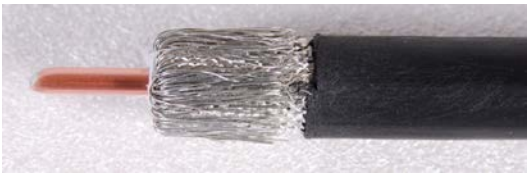
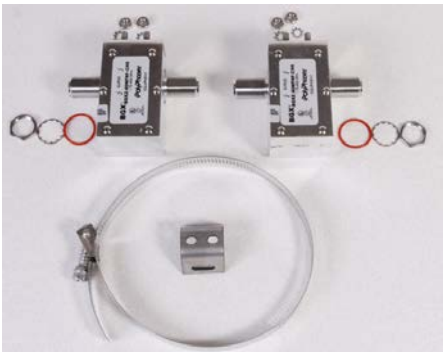
Cambium part number	Standard	Sub-band	Sub-band frequency	T/R spacing
01010433002	FCC	B1-Lo	38595 – 38805 MHz	700 MHz
01010433003		B1-Hi	39295 – 39505 MHz	
01010433004		B2-Lo	38795 – 39005 MHz	
01010433005		B2-Hi	39495 – 39705 MHz	
01010433006		B3-Lo	38995 – 39205 MHz	
01010433007		B3-Hi	39695 – 39905 MHz	
01010433008		B4-Lo	39195 – 39405 MHz	
01010433009		B4-Hi	39895 – 40105 MHz	
01010433010	ETSI	B1-Lo	37044 – 37632 MHz	1260 MHz
01010433011		B1-Hi	38304 – 38892 MHz	
01010433012		B2-Lo	37604 – 38192 MHz	
01010433001		B2-Hi	38864 – 39452 MHz	

Ordering IF cable, grounding and LPUs

NOTE
Applies to ODU deployments only.

For ODU based installations, select cable and LPU components from Table 56.

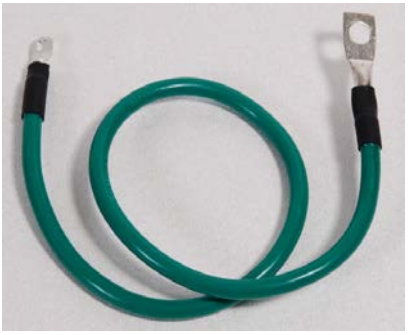
Table 56 Cable and LPU components

Item	Cambium part number and notes
CNT-400 coaxial cable, 50 Ohm (IF cable) 	CNT-400 cable is supplied by Cambium with the following lengths and part numbers. '50 Ohm Braided Coaxial Cable - 75 meter'. Cambium part number 30010194001. '50 Ohm Braided Coaxial Cable - 500 meter'. Cambium part number 30010195001. For 1+1 and 2+0 links, order enough IF cable to connect two ODU/CMU pairs at each link end.
Lightning protection unit (LPU) end kit 	Quantity per link: 1+0 links: 2 LPU kits (4 LPUs). 1+1 Hot Standby links: 4 LPU kits (8 LPUs). 2+0 links: 4 LPU kits (8 LPUs). 'LPU END KIT PTP800'. Cambium part number WB3657.
Hoisting Grip for CNT-400 cable 	For hoisting the IF cable up to the ODU without damaging the connector. Quantity per link: 1+0 links: 2 minimum. 1+1 Hot Standby links: 4 minimum. 2+0 links: 4 minimum. 'Hoisting Grip for CNT-400 cable'. Cambium part number 07009304001.

Item	Cambium part number and notes
Coaxial cable installation assembly kit (for CNT-400 cable) 	Quantity per link: 1+0 links: 2 kits. 1+1 Hot Standby links: 4 kits. 2+0 links: 4 kits. 'Coaxial Cable Installation Assembly Kit'. Cambium part number WB3616. For kit contents, see Table 57.
Cable grounding kits for 1/4" and 3/8" cable 	Additional grounding kits may be required to cover all IF cable grounding points. 'Cable Grounding Kits For 1/4" And 3/8" Cable'. Cambium part number 01010419001. Kit contents: grounding cable, self-amalgamating tape, PVC tape, tie-wraps, bolts, washers and nuts.
Crimp tool for N-type connector 	Required for crimping N-type connectors to IF cables. 'Crimp tool for N-type connector'. Cambium part number 66010063001.

Table 57 Inventory of the coaxial cable installation assembly kit (WB3616)

Item	Notes
Braided cable assembly 	Quantity per kit: 1. 0.7 meter long cable to go between the ODU and the top LPU.
Cable grounding kits for 1/4" and 3/8" cable 	Quantity per kit: 2. Each kit contains, earth wire, PVC tape, self amalgamating tape and fixings.
Ground lead 	Quantity per kit: 1 Green, 0.8 meter long with M5 lugs fitted each end. Use for grounding the ODU to the top LPU.

Item	Notes
Ground lead 	Quantity per kit: 2. Green, 0.6 meter long with M5 lugs fitted one end and M10 the other. Use for grounding the top and bottom LPUs to the supporting structure.
Weather proofing kit 	Quantity per kit: 1. Kit contains 6 reels of self amalgamating tape, 2 reels of 19mm wide PVC tape and 1 reel of 50mm wide PVC tape.
N type connector 	Quantity per kit: 4. To fit CNT-400 cable. Use crimp tool part number 66010063001.
Cable ties 	Quantity per kit: 50.

Ordering RMKs and waveguides

> **NOTE**
> Applies to ODU deployments only.

For remote mounted ODUs (or couplers) select RMKs, waveguides and accessories from Table 58.

Table 58 RMKs, waveguides and accessories

Item	Cambium part number and notes
ODU remote mounting kit 	Quantity per remote mounted ODU: 1. Part numbers: listed in Table 59.
Flexible waveguide 	Quantity per remote mounted ODU: 1. Part numbers: listed in Table 60. All waveguides are 900 mm (35 in) long. For more information, see Flexible waveguide specifications on page 4-10.
Flex-twist hanger kit 	Quantity per remote mounted ODU: 2. Part numbers: listed in Table 61. To provide adequate support for a 900mm flexible waveguide, two hangers are required.

Item	Cambium part number and notes
Tapered transition 	Required only for 11 GHz remote-mounted antennas, fitted between the antenna and the flexible waveguide. Quantity per remote mounted ODU: 1. Part number: 58010077001. For more information, see Flexible waveguide specifications on page 4-10.

Table 59 Remote mounting kits

Band	Output	Cambium part number
6 GHZ	UDR70	07010109008
7 GHz	UBR84	07010109001
8 GHz	UBR84	07010109002
11 – 13 GHZ	UBR120	07010109003
15 GHz	UBR140	07010109004
18 – 26 GHz	UBR220	07010109005
28 – 32 GHz	UBR320	07010109006
38 GHz	UBR320	07010109007

Table 60 Flexible waveguides

Band	Cambium part number	Atten-uation	VSWR	Flanges (RMK/ antenna)	Max twist	Min bend radius (E/H plane)
6 GHz	58010076016	0.3 dB/m	1.10	PDR70 CPR137G	214°/m	E: 102 mm (4.0 in) H: 204 mm (8.0 in)
6 GHz	58010076017	0.3 dB/m	1.10	PDR70 UDR70	214°/m	E: 102 mm (4.0 in) H: 204 mm (8.0 in)
7 GHz 8 GHz	58010076019	0.4 dB/m	1.10	PBR84 UDR84	264°/m	E: 76 mm (3.0 in) H: 152 mm (6.0 in)
11 GHz 13 GHz	58010076005	0.6 dB/m	1.10	PBR120 UBR120	360°/m	E: 64 mm (2.5 in) H: 115 mm (4.5 in)
11 GHz 13 GHz	58010076018			PDR100 CPR90G		
15 GHz	58010076008	0.99 dB/m	1.10	PBR140 UBR140	445°/m	E: 52 mm (2 in) H: 102 mm (4 in)
18 GHz 23 GHz 26 GHz	58010076011	2.6 dB/m	1.25	PBR220 UBR220	510°/m	E: 38 mm (1.5 in) H: 76 mm (3.0 in)
28 GHz 32 GHz 38 GHz	58010076014	3.3 dB/m	1.30	PBR320 UBR320	510°/m	E: 38 mm (1.5 in) H: 76 mm (3.0 in)

Table 61 Flex-twist hanger kits available from Cambium

Accessory	Frequency variant	Cambium part number
WR137 flex-twist hanger kit	6 GHz	07010118001
WR112 flex-twist hanger kit	7 – 8 GHz	07010118002
WR75 flex-twist hanger kit	11 – 13 GHz	07010118003
WR62 flex-twist hanger kit	15 GHz	07010118004
WR42 flex-twist hanger kit	18 – 26 GHz	07010118005
WR28 flex-twist hanger kit	28 – 38 GHz	07010118006

Ordering coupler mounting kits

NOTE
Applies to ODU deployments only.

Determine the number of coupler mounting kits required per link, as follows:

- 1+0 links: not required.
- 1+1 Hot Standby links without antenna protection: 2 coupler mounting kits.
- 1+1 Hot Standby links with antenna protection: not required.
- 2+0 co-polar links: 2 coupler mounting kits.
- 2+0 cross-polar links: not required.

Select symmetric or asymmetric couplers.

Select coupler mounting kits from Table 62.

Table 62 ODU coupler mounting kits

Band	Coupler type	Cambium part number
6 GHz	3 dB symmetric	07010110021
6 GHz	6 dB asymmetric	07010110022
7 GHz	3 dB symmetric	07010110001
7 GHz	6 dB asymmetric	07010110002

Band	Coupler type	Cambium part number
8 GHz	3 dB symmetric	07010110003
8 GHz	6 dB asymmetric	07010110004
11 GHz	3 dB symmetric	07010110005
11 GHz	6 dB asymmetric	07010110006
13 GHz	3 dB symmetric	07010110007
13 GHz	6 dB asymmetric	07010110008
15 GHz	3 dB symmetric	07010110009
15 GHz	6 dB asymmetric	07010110010
18 GHz	3 dB symmetric	07010110011
18 GHz	6 dB asymmetric	07010110012
23 GHz	3 dB symmetric	07010110013
23 GHz	6 dB asymmetric	07010110014
26 GHz	3 dB symmetric	07010110015
26 GHz	6 dB asymmetric	07010110016
28 GHz	3 dB symmetric	07010110023
28 GHz	6 dB asymmetric	07010110024
32 GHz	3 dB symmetric	07010110017
32 GHz	6 dB asymmetric	07010110018
38 GHz	3 dB symmetric	07010110019
38 GHz	6 dB asymmetric	07010110020

Ordering OMKs

NOTE
Applies to ODU deployments only.

To upgrade any standard antenna to support a direct mount interface in a 2+0 cross-polar link, purchase an orthogonal mount kit (OMK). Select an OMK that is in the same band as the antenna that it is upgrading; for example, use a 6 GHz OMK to upgrade a 6 GHz antenna. Select OMKs from Table 63.

Table 63 Orthogonal mounting kits (OMKs)

Band	Cambium part number
6 GHz	85009316001
7 GHz and 8 GHz	85009316002
11 GHz	85009316004
13 GHz	85009316005
15 GHz	85009316006
18 GHz	85009316007
23 GHz	85009316008

NOTE
Cambium also supply dual-polar direct mount antennas complete with orthogonal mode transducers for 2+0 cross-polar links. See Ordering antennas on page 2-59.

Ordering IRFUs and accessories

> **NOTE**
> Applies to IRFU deployments only.

Select IRFUs and IRFU accessories from the following tables:

- IRFUs (6 GHz and 11 GHz): Table 64.
- IF cable between IRFU and CMU: Table 65.
- IRFU transceivers, fan and covers (6 GHz and 11 GHz): Table 66.
- RF cables between transceiver and BU (6 GHz and 11 GHz): Table 67.
- IRFU filter assemblies (6 GHz and 11 GHz): Table 68.
- IRFU upgrade kits (6 GHz and 11 GHz): Table 69.
- Antennas and antenna accessories for IRFU deployments: Table 70.

> **NOTE**
> When ordering IRFUs, specify the Tx and Rx center frequencies.

Table 64 IRFUs – 6 GHz and 11 GHz

Cambium number	Description
58009282002	IRFU,ANSI,6G,1+0,HP
58009282013	IRFU,ANSI,6G,1+0 MHSB Ready to upgrade to 1+1,EQ,HP
58009282014	IRFU,ANSI,6G,1+0 MHSB Ready to upgrade to 1+1,UNEQ,HP
58009282005	IRFU,ANSI,6G,1+1,EQ,HP
58009282006	IRFU,ANSI,6G,1+1,UNEQ,HP
58009282004	IRFU,ANSI,6G,1+1 with SD,HP
58009282007	IRFU,ANSI,6G,2+0,HP
58009281002	IRFU,ANSI,11G,1+0,10/30MHz,HP
58009281019	IRFU,ANSI,11G,1+0 MHSB Ready to upgrade to 1+1,EQ,10/30MHz,HP
58009281021	IRFU,ANSI,11G,1+0 MHSB Ready to upgrade to 1+1,UNEQ,10/30MHz,HP
58009281004	IRFU,ANSI,11G,1+1,EQ,10/30MHz,HP
58009281006	IRFU,ANSI,11G,1+1,UNEQ,10/30MHz,HP

Cambium number	Description
58009281008	IRFU,ANSI,11G,1+1 with SD,10/30MHz,HP
58009281010	IRFU,ANSI,11G,2+0,10/30MHz,HP
58009281003	IRFU,ANSI,11G,1+0,40MHz,HP
58009281020	IRFU,ANSI,11G,1+0 MHSB Ready to upgrade to 1+1,EQ,40MHz,HP
58009281022	IRFU,ANSI,11G,1+0 MHSB Ready to upgrade to 1+1,UNEQ,40MHz,HP
58009281005	IRFU,ANSI,11G,1+1,EQ,40MHz,HP
58009281005	IRFU,ANSI,11G,1+1,EQ,40MHz,HP
58009281007	IRFU,ANSI,11G,1+1,UNEQ,40MHz,HP
58009281009	IRFU,ANSI,11G,1+1 with SD,40MHz,HP
58009281011	IRFU,ANSI,11G,2+0,40MHz,HP
58009281032	IRFU,ANSI,Side A "6G,1+0,HP" and Side B "6G,1+0,HP"
58009281030	IRFU,ANSI,Side A "6G,1+0,HP" and Side B "11G,1+0,10/30 MHz,HP"
58009281031	IRFU,ANSI,Side A "6G,1+0,HP" and Side B "11G,1+0,40 MHz,HP"
58009281027	IRFU,ANSI,Side A "11G,1+0,10/30 MHz,HP" and Side B "11G,1+0,10/30 MHz,HP"
58009281028	IRFU,ANSI,Side A "11G,1+0,10/30 MHz,HP" and Side B "11G,1+0,40 MHz,HP"
58009281029	IRFU,ANSI,Side A "11G,1+0,40 MHz,HP" and Side B "11G,1+0,40 MHz,HP"

Table 65 IF cable between IRFU and CMU

Cambium number	Description
30009403001	IF cable for CMU and IRFU

Table 66 IRFU transceivers, fan and covers – 6 GHz and 11 GHz

Cambium number	Description
58009282001	XCVR,ANSI,6G,HP
58009281001	XCVR,ANSI,11G,HP
64009324003	FAN Assembly of IRFU
64009324001	IRFU Shelf Frontal Cover
64009324002	IRFU Shelf Frontal Extended Cover

Table 67 RF cables between transceiver and BU – 6 GHz and 11 GHz

Cambium number	Description
30009399001	Cable Assembly Kit 1, SMA, M-M, R/A
30009399004	Cable Assembly Kit 2, SMA, M-M, R/A
30009399005	Cable Assembly Kit 3, SMA, M-M, R/A
30009399006	Cable Assembly Kit 4, SMA, M-M, R/A
30009399007	Cable Assembly Kit 5, SMA, M-M, R/A
30009399008	Cable Assembly Kit 6, SMA, M-M, R/A
30009399009	Cable Assembly Kit 7, SMA, M-M, R/A
30009399010	Cable Assembly Kit 8, SMA, M-M, R/A
30009399011	Cable Assembly Kit 9, SMA, M, R/A-M, R/A
30009399002	Cable Assembly Kit 10, SMA, M, R/A-M, R/A
30009399003	Cable Assembly Kit 11, SMA, M, R/A-M, R/A

Table 68 IRFU filter assemblies – 6 GHz and 11 GHz

Cambium number	Description
91009315001 (*)	Tx Filter Assembly,6G, 10/30MHz
91009315004 (*)	Rx Filter Assembly,6G, 10/30MHz
91009315002 (*)	Tx Filter Assembly,11G, 40 MHz
91009315003 (*)	Tx Filter Assembly,11G, 10/30MHz
91009315005 (*)	Rx Filter Assembly,11G, 40 MHz
91009315006 (*)	Rx Filter Assembly,11G, 10/30MHz

(*) When ordering these filter assemblies, specify central frequency.

Table 69 IRFU upgrade kits – 6 GHz and 11 GHz

Cambium number	Description
58009282008	IRFU,ANSI,6G,EQ,HP, 1+0 to 1+1 MHSB Upgrade Kit
58009282009	IRFU,ANSI,6G,UNEQ,HP,1+0 to 1+1 MHSB Upgrade Kit
58009282011	IRFU,ANSI,6G,HP,1+0 MHSB Ready to 1+1 MHSB Upgrade Kit
58009282012 (*)	IRFU,ANSI,6G,HP,1+0 MHSB Ready to 1+1 MHSB with SD Upgrade Kit
58009282010 (*)	IRFU,ANSI,6G,HP,1+0 to 1+1 MHSB with SD Upgrade Kit
58009281014	IRFU,ANSI,11G,EQ,HP, 1+0 to 1+1 MHSB Upgrade Kit
58009281015	IRFU,ANSI,11G,UNEQ,HP,1+0 to 1+1 MHSB Upgrade Kit
58009281017	IRFU,ANSI,11G,HP,1+0 MHSB Ready to 1+1 MHSB Upgrade Kit
58009281018 (*)	IRFU,ANSI,11G,HP,1+0 MHSB Ready to 1+1 MHSB with SD Upgrade Kit,10/30 MHz
58009281016 (*)	IRFU,ANSI,11G,HP,1+0 to 1+1 MHSB with SD Upgrade Kit,10/30 MHz
58009281025 (*)	IRFU,ANSI,11G,HP,1+0 MHSB Ready to 1+1 MHSB with SD Upgrade Kit,40 MHz
58009281026 (*)	IRFU,ANSI,11G,HP,1+0 to 1+1 MHSB with SD Upgrade Kit,40 MHz

(*) When ordering these kits, specify Rx center frequency.

Table 70 Antennas and antenna accessories for IRFU deployments

Cambium number	Description
58009273001	EWP52 - Premium Elliptical Waveguide, 5.725 - 6.425 GHz (per ft)
58009273003	EWP63 - Premium Elliptical Waveguide, 6.425 - 7.125 GHz (per ft)
58009273002	EWP90 - Premium Elliptical Waveguide, 10.7 - 11.7 GHz (per ft)
09009399001	Fixed-tuned CPR137G connector for EWP52
09009399003	Fixed-tuned CPR137G connector for EWP63
09009399002	Fixed-tuned CPR90G connector for EWP90
07009343002	Grounding Kit for waveguide EWP90
07009343001	Grounding Kit for waveguide EWP52 and EWP63
07009344001	Hoisting Grip for waveguide EWP52 and EWP63
07009344002	Hoisting Grip for waveguide EWP90
58009283001	Pressure Window for WR137, 5.85-8.2 GHz, mates to CPR137G
58009283002	Pressure Window for WR90, 8.2-12.4 GHz, mates to CPR90G
01009504002	DryLine Dehydrator, Low-pressure membrane, Wall Mountable, 115 Vac
58009284001	2-port Gas Distribution Manifold
58009284002	4-port Gas Distribution Manifold
58009279001	1' Flex Waveguide 11 GHz - CRP90G/CRP90G
58009279002	2' Flex Waveguide 11 GHz - CRP90G/CRP90G
58009279003	3' Flex Waveguide 11 GHz - CRP90G/CRP90G
58009280001	1' Flex Waveguide 6 GHz - CRP137G/CRP137G
58009280002	2' Flex Waveguide 6 GHz - CRP137G/CRP137G
58009280003	3' Flex Waveguide 6 GHz - CRP137G/CRP137G
85009328001 (*)	HP4 - 4' SP Antenna, 5.725 ~ 6.425 GHz with radome, Single Pol, CPR137G
85009328002 (*)	HP4 - 4' SP Antenna, 6.425 ~ 7.125 GHz with radome, Single Pol, CPR137G

(*) Required for Receive Spatial Diversity only.

Ordering network connection components

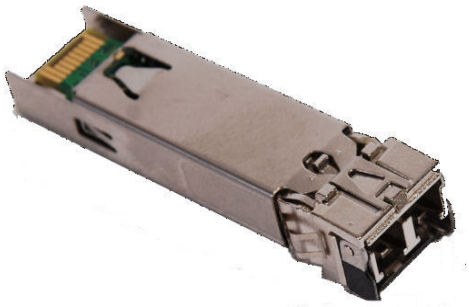
Select network connection components from Table 71 (copper interfaces) or Table 72 (fiber interfaces).

Table 71 Copper network cables and connectors

Item	Cambium part number and notes
Screened Cat5e cable	To minimise radiated emissions, use screened Cat5e cable for all copper connections from the CMU Ethernet ports (Data or Management) to any network switch.
RJ45 connectors	Two required per Cat5e cable.
Out-of-band protection splitter 	Quantity per link: 2 (with out-of-band management). Only required for 1+1 links with out-of-band management. '1+1 Out-of-Band Splitter Kit'. Cambium part number WB3807.
Protection cable	Quantity per link: 2 (with in-band management). Only required for 1+1 links with in-band management. For specification, see Protection cable on page 4-17.

Table 72 Fiber network cables and connectors

Item	Cambium part number and notes
Fiber cable and connectors	If a fiber interface between the CMU and Ethernet switch is required, then fiber cable and connectors are needed (not supplied by Cambium).

Item	Cambium part number and notes
SFP Gig-E fiber pluggable module 	If a fiber interface between the CMU and Ethernet switch is required, then two SFP modules are needed. Either: 'SFP SX Gig-E Optical Pluggable Module - 850 nm'. Cambium part number 01010430001. Or: 'SFP LX Gig-E Optical Pluggable Module - 1310 nm'. Cambium part number 01010431001.
Fiber-Y kit 	Optional customer network connection for a 1+1 Hot Standby link with out-of-band management. Quantity per link: 2 (with out-of-band management). '1+1 Optical-Y Splitter Kit per end (inc SFP Modules - 850nm)'. Cambium part number WB3806. Kit contains: Two Optical-Y cable assemblies (one illustrated), one for transmit and one for receive. Two 1000-BASE-SX SFP modules.

Ordering capacity upgrades

NOTE

Purchasing a capacity upgrade will not necessarily lead to an increase in data capacity, as capacity also depends on channel bandwidth and modulation mode. For more information, see Capacity, transmit power and sensitivity on page 4-22.

Select either a single-step capacity upgrade from Table 73, or one or more step-by-step capacity upgrades from Table 74.

Table 73 Single-step capacity upgrades (per unit)

Cambium part	Capacity
WB3538	20 Mbps
WB3539	30 Mbps
WB3540	40 Mbps
WB3541	50 Mbps
WB3542	100 Mbps
WB3543	150 Mbps
WB3544	200 Mbps
WB3545	300 Mbps
WB3546	Full capacity

Table 74 Step-by-step capacity upgrades (per unit)

Cambium part	Capacity increase
WB3547	20 Mbps → 30 Mbps
WB3548	30 Mbps → 40 Mbps
WB3549	40 Mbps → 50 Mbps
WB3550	50 Mbps → 100 Mbps
WB3551	100 Mbps → 150 Mbps
WB3552	150 Mbps → 200 Mbps
WB3553	200 Mbps → 300 Mbps
WB3554	300 Mbps → full capacity

Chapter 3: Legal information

This chapter provides legal notices including software license agreements.

⚠ CAUTION

Changes or modifications must not be made to the equipment without the express consent of the party responsible for compliance. Any such modifications could void the user's authority to operate the equipment and will void the manufacturer's warranty.

The following topics are described in this section:

- Cambium Networks end user license agreement on page 3-2
- Hardware warranty on page 3-20
- Limit of liability on page 3-21

Cambium Networks end user license agreement

Acceptance of this agreement

In connection with Cambium's delivery of certain proprietary software or products containing embedded or pre-loaded proprietary software, or both, Cambium is willing to license this certain proprietary software and the accompanying documentation to you only on the condition that you accept all the terms in this End User License Agreement ("Agreement").

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT USE THE PRODUCT OR INSTALL THE SOFTWARE. INSTEAD, YOU MAY, FOR A FULL REFUND, RETURN THIS PRODUCT TO THE LOCATION WHERE YOU ACQUIRED IT OR PROVIDE WRITTEN VERIFICATION OF DELETION OF ALL COPIES OF THE SOFTWARE. ANY USE OF THE SOFTWARE, INCLUDING BUT NOT LIMITED TO USE ON THE PRODUCT, WILL CONSTITUTE YOUR ACCEPTANCE TO THE TERMS OF THIS AGREEMENT.

Definitions

In this Agreement, the word "Software" refers to the set of instructions for computers, in executable form and in any media, (which may include diskette, CD-ROM, downloadable internet, hardware, or firmware) licensed to you. The word "Documentation" refers to electronic or printed manuals and accompanying instructional aids licensed to you. The word "Product" refers to Cambium's fixed wireless broadband devices for which the Software and Documentation is licensed for use.

Grant of license

Cambium Networks Limited ("Cambium") grants you ("Licensee" or "you") a personal, nonexclusive, non-transferable license to use the Software and Documentation subject to the Conditions of Use set forth in "Conditions of use" and the terms and conditions of this Agreement. Any terms or conditions relating to the Software and Documentation appearing on the face or reverse side of any purchase order, purchase order acknowledgment or other order document that are different from, or in addition to, the terms of this Agreement will not be binding on the parties, even if payment is accepted.

Conditions of use

Any use of the Software and Documentation outside of the conditions set forth in this Agreement is strictly prohibited and will be deemed a breach of this Agreement.

1. Only you, your employees or agents may use the Software and Documentation. You will take all necessary steps to insure that your employees and agents abide by the terms of this Agreement.

2. You will use the Software and Documentation (i) only for your internal business purposes; (ii) only as described in the Software and Documentation; and (iii) in strict accordance with this Agreement.

3. You may use the Software and Documentation, provided that the use is in conformance with the terms set forth in this Agreement.

4. Portions of the Software and Documentation are protected by United States copyright laws, international treaty provisions, and other applicable laws. Therefore, you must treat the Software like any other copyrighted material (for example, a book or musical recording) except that you may either: (i) make 1 copy of the transportable part of the Software (which typically is supplied on diskette, CD-ROM, or downloadable internet), solely for back-up purposes; or (ii) copy the transportable part of the Software to a PC hard disk, provided you keep the original solely for back-up purposes. If the Documentation is in printed form, it may not be copied. If the Documentation is in electronic form, you may print out 1 copy, which then may not be copied. With regard to the copy made for backup or archival purposes, you agree to reproduce any Cambium copyright notice, and other proprietary legends appearing thereon. Such copyright notice(s) may appear in any of several forms, including machine-readable form, and you agree to reproduce such notice in each form in which it appears, to the extent it is physically possible to do so. Unauthorized duplication of the Software or Documentation constitutes copyright infringement, and in the United States is punishable in federal court by fine and imprisonment.

5. You will not transfer, directly or indirectly, any product, technical data or software to any country for which the United States Government requires an export license or other governmental approval without first obtaining such license or approval.

Title and restrictions

If you transfer possession of any copy of the Software and Documentation to another party outside of the terms of this agreement, your license is automatically terminated. Title and copyrights to the Software and Documentation and any copies made by you remain with Cambium and its licensors. You will not, and will not permit others to: (i) modify, translate, decompile, bootleg, reverse engineer, disassemble, or extract the inner workings of the Software or Documentation, (ii) copy the look-and-feel or functionality of the Software or Documentation; (iii) remove any proprietary notices, marks, labels, or logos from the Software or Documentation; (iv) rent or transfer all or some of the Software or Documentation to any other party without Cambium's prior written consent; or (v) utilize any computer software or hardware which is designed to defeat any copy protection device, should the Software and Documentation be equipped with such a protection device. If the Software and Documentation is provided on multiple types of media (such as diskette, CD-ROM, downloadable internet), then you will only use the medium which best meets your specific needs, and will not loan, rent, lease, or transfer the other media contained in the package without Cambium's written consent. Unauthorized copying of the Software or Documentation, or failure to comply with any of the provisions of this Agreement, will result in automatic termination of this license.

Confidentiality

You acknowledge that all Software and Documentation contain valuable proprietary information and trade secrets and that unauthorized or improper use of the Software and Documentation will result in irreparable harm to Cambium for which monetary damages would be inadequate and for which Cambium will be entitled to immediate injunctive relief. If applicable, you will limit access to the Software and Documentation to those of your employees and agents who need to use the Software and Documentation for your internal business purposes, and you will take appropriate action with those employees and agents to preserve the confidentiality of the Software and Documentation, using the same degree of care to avoid unauthorized or improper disclosure as you use for the protection of your own proprietary software, but in no event less than reasonable care.

You have no obligation to preserve the confidentiality of any proprietary information that: (i) was in the public domain at the time of disclosure; (ii) entered the public domain through no fault of yours; (iii) was given to you free of any obligation to keep it confidential; (iv) is independently developed by you; or (v) is disclosed as required by law provided that you notify Cambium prior to such disclosure and provide Cambium with a reasonable opportunity to respond.

Right to use Cambium's name

Except as required in "Conditions of use", you will not, during the term of this Agreement or thereafter, use any trademark of Cambium Networks, or any word or symbol likely to be confused with any Cambium Networks trademark, either alone or in any combination with another word or words.

Transfer

The Software and Documentation may not be transferred to another party without the express written consent of Cambium, regardless of whether or not such transfer is accomplished by physical or electronic means. Cambium's consent may be withheld at its discretion and may be conditioned upon transferee paying all applicable license fees and agreeing to be bound by this Agreement.

Updates

During the first 12 months after purchase of a Product, or during the term of any executed Maintenance and Support Agreement for the Product, you are entitled to receive Updates. An "Update" means any code in any form which is a bug fix, patch, error correction, or minor enhancement, but excludes any major feature added to the Software. Updates are available for download at the support website.

Major features may be available from time to time for an additional license fee. If Cambium makes available to you major features and no other end user license agreement is provided, then the terms of this Agreement will apply.

Maintenance

Except as provided above, Cambium is not responsible for maintenance or field service of the Software under this Agreement.

Disclaimer

CAMBIUM DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR IN ANY COMMUNICATION WITH YOU. CAMBIUM SPECIFICALLY DISCLAIMS ANY WARRANTY INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILTY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS." CAMBIUM DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. CAMBIUM MAKES NO WARRANTY WITH RESPECT TO THE CORRECTNESS, ACCURACY, OR RELIABILITY OF THE SOFTWARE AND DOCUMENTATION. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Limitation of liability

THE TOTAL LIABILITY OF CAMBIUM UNDER THIS AGREEMENT FOR DAMAGES WILL NOT EXCEED THE TOTAL AMOUNT PAID BY YOU FOR THE PRODUCT LICENSED UNDER THIS AGREEMENT. IN NO EVENT WILL CAMBIUM BE LIABLE IN ANY WAY FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL OR PUNITIVE DAMAGES OF ANY NATURE, INCLUDING WITHOUT LIMITATION, LOST BUSINESS PROFITS, OR LIABILITY OR INJURY TO THIRD PERSONS, WHETHER FORESEEABLE OR NOT, REGARDLESS OF WHETHER CAMBIUM HAS BEEN ADVISED OF THE POSSIBLITY OF SUCH DAMAGES. Some jurisdictions do not permit limitations of liability for incidental or consequential damages, so the above exclusions may not apply to you.

U.S. government

If you are acquiring the Product on behalf of any unit or agency of the U.S. Government, the following applies. Use, duplication, or disclosure of the Software and Documentation is subject to the restrictions set forth in subparagraphs (c) (1) and (2) of the Commercial Computer Software – Restricted Rights clause at FAR 52.227-19 (JUNE 1987), if applicable, unless being provided to the Department of Defense. If being provided to the Department of Defense, use, duplication, or disclosure of the Products is subject to the restricted rights set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT 1988), if applicable. Software and Documentation may or may not include a Restricted Rights notice, or other notice referring specifically to the terms and conditions of this Agreement. The terms and conditions of this Agreement will each continue to apply, but only to the extent that such terms and conditions are not inconsistent with the rights provided to you under the aforementioned provisions of the FAR and DFARS, as applicable to the particular procuring agency and procurement transaction.

Term of license

Your right to use the Software will continue in perpetuity unless terminated as follows. Your right to use the Software will terminate immediately without notice upon a breach of this Agreement by you. Within 30 days after termination of this Agreement, you will certify to Cambium in writing that through your best efforts, and to the best of your knowledge, the original and all copies, in whole or in part, in any form, of the Software and all related material and Documentation, have been destroyed, except that, with prior written consent from Cambium, you may retain one copy for archival or backup purposes. You may not sublicense, assign or transfer the license or the Product, except as expressly provided in this Agreement. Any attempt to otherwise sublicense, assign or transfer any of the rights, duties or obligations hereunder is null and void.

Governing law

This Agreement is governed by the laws of the United States of America to the extent that they apply and otherwise by the laws of the State of Illinois.

Assignment

This agreement may not be assigned by you without Cambium's prior written consent.

Survival of provisions

The parties agree that where the context of any provision indicates an intent that it survives the term of this Agreement, then it will survive.

Entire agreement

This agreement contains the parties' entire agreement regarding your use of the Software and may be amended only in writing signed by both parties, except that Cambium may modify this Agreement as necessary to comply with applicable laws.

Third party software

The software may contain one or more items of Third-Party Software supplied by other third-party suppliers. The terms of this Agreement govern your use of any Third-Party Software UNLESS A SEPARATE THIRD-PARTY SOFTWARE LICENSE IS INCLUDED, IN WHICH CASE YOUR USE OF THE THIRD-PARTY SOFTWARE WILL THEN BE GOVERNED BY THE SEPARATE THIRD-PARTY LICENSE.

OpenSSL

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)".

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

NET SNMP

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or withoutmodification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2008, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Explorer Canvas JavaScript Library

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

Hardware warranty

Cambium’s standard hardware warranty is for one (1) year from date of shipment from Cambium or a Cambium Point-To-Point Distributor. Cambium warrants that hardware will conform to the relevant published specifications and will be free from material defects in material and workmanship under normal use and service. Cambium shall within this time, at its own option, either repair or replace the defective product within thirty (30) days of receipt of the defective product. Repaired or replaced product will be subject to the original warranty period but not less than thirty (30) days.

Limit of liability

IN NO EVENT SHALL CAMBIUM NETWORKS BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF CAMBIUM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.) IN NO CASE SHALL CAMBIUM'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

Chapter 4: Reference information

This chapter describes the physical, environmental, safety, wireless and electromagnetic specifications for PTP 800.

The following topics are described in this chapter:

- Equipment specifications on page 4-2 contains specifications of the CMU, RFU and other equipment supplied by Cambium for PTP 800 installations.
- Wireless specifications on page 4-19 contains specifications of the PTP 800 wireless interface, including RF bands, channel width and link loss.
- Data network specifications on page 4-71 contains specifications of the PTP 800 Ethernet interface.
- Syslog message formats on page 4-73 describes the format and content of Syslog event messages.
- Network management specifications on page 4-77 lists supported SNMP objects from the standard MIB-II, IF-MIB and Bridge-MIB.
- Electromagnetic compliance on page 4-82 describes how the PTP 800 complies with the regulations that are in force in various countries, and contains notifications made to regulatory bodies for the PTP 800.
- Radiation hazard assessment on page 4-86 evaluates the radiation levels produced by the PTP 800 products against ETSI and FCC standards.

Equipment specifications

This section contains specifications of the CMU, RFU and other equipment supplied by Cambium for PTP 800 installations.

CMU specifications

The PTP 800 CMU (Cambium part number WB3480) conforms to the specifications listed in Table 75, Table 76 and Table 77. The CMU and ODU power consumption figures are specified in Table 78.

Table 75 CMU physical specifications

Category	Specification
Dimensions	Width 18.0 cm (7.1 in), Height 3.5 cm (1.4 in), Depth 22.0 cm (8.7 in)
Weight	1.1 kg (2.4 lbs)

Table 76 CMU environmental specifications

Category	Specification
Temperature	–33°C to 55°C
Humidity	95% non-condensing
Waterproof	IP20
UV Exposure	10 year operational life (UL746C test evidence)

Table 77 CMU electrical specifications

Category	Specification
Input voltage	–40.5 V to –60 V
Input voltage withstand	0 V to –72 V
CMU dissipation	21 W

Table 78 ODU and CMU power consumption (ODU-A only)

Band (GHz)	ODU in Mute (W) (*1)	ODU in Transmit (W) (*2)	CMU (W)	1+0 Configuration (W)	1+1 Configuration (W)
6	29	46	20	66	115
7	29	46	20	66	115
8	29	46	20	66	115
11	23	46	20	66	109
13	10	35	20	55	85
15	10	35	20	55	85
18	7	35	20	55	82
23	14	35	20	55	89
26	14	35	20	55	89
28	13	35	20	55	88
32	19	35	20	55	94
38	21	35	20	55	96

(*1) Typical ODU DC power consumption in Mute condition (W)

(*2)Typical ODU DC power consumption in Transmit condition (W)

AC to DC converter specifications

For details of alternative power supply arrangements, refer to Power supply considerations on page 2-4.

The PTP 800 AC to DC converter conforms to the specifications listed in Table 79.

Table 79 AC to DC converter specifications

Category	Specification
Input range	90 to 264 V ac (wide range)
Output voltage	Single output 48 V dc nominal
Maximum output power	80 W
Line frequency	47 to 63 Hz
Inrush current	40 A maximum at 264 V ac, cold start 25 °C
Input current	1.8 A maximum
Power conversion efficiency	85% typical
Electromagnetic compatibility	FCC Part 15, Subpart B Class A EN55022 (CISPR 22) Class A
Safety ground leakage current	3.5 mA maximum at 60 Hz, 254 V ac input
Hold-up time	10 ms minimum at full load at 90/264 V ac
Overvoltage protection	53 - 60 V latching type, recycle ac to reset
Overcurrent protection	Output short-circuit protection automatic recovery
Thermal protection	Output will latch off
Waterproof	IP20
Temperature	–33°C to 55°C

ODU specifications

The PTP 800 ODU conforms to the specifications listed in Table 80 and Table 81.

Table 80 ODU physical specifications

Category	ODU-A	ODU-B
Dimensions	Diameter 26.7 cm (10.5 in), Depth 8.9 cm (3.5 in)	Diameter 25.2 cm (9.9 in), Depth 9.2 cm (3.6 in)
Weight	4.6 kg (10.1 lbs)	3.9 kg (8.6 lbs)

Table 81 ODU-A and ODU-B environmental specifications

Category	Specification
Temperature	–33°C to 55°C (cold start at -45°C)
Humidity	100% condensing
Waterproof	IP67
UV Exposure	10 year operational life (UL746C test evidence)

RSSI output

Table 82 specifies the voltage measured at the RSSI connector of the ODU for each combination of received signal level (dBm) and channel separation or bandwidth (MHz). This table applies to ODU-A and ODU-B.

Table 82 RSSI voltage, received signal level and bandwidth

RSL (dBm)	Channel separation 7, 13.75, 14, 27.5, 28, 29.65, 55, 56, 60 or 80 MHz	Bandwidth 10, 20 or 40 MHz	Bandwidth 30 MHz	Bandwidth 50 MHz
-20	4.54	4.63	4.71	4.57
-21	4.48	4.57	4.65	4.51
-22	4.41	4.50	4.58	4.44
-23	4.35	4.44	4.52	4.38
-24	4.29	4.38	4.46	4.32

RSL (dBm)	Channel separation 7, 13.75, 14, 27.5, 28, 29.65, 55, 56, 60 or 80 MHz	Bandwidth 10, 20 or 40 MHz	Bandwidth 30 MHz	Bandwidth 50 MHz
-25	4.22	4.31	4.39	4.25
-26	4.16	4.25	4.33	4.19
-27	4.10	4.19	4.27	4.13
-28	4.03	4.12	4.20	4.06
-29	3.97	4.06	4.14	4.00
-30	3.90	4.00	4.08	3.94
-31	3.84	3.93	4.01	3.87
-32	3.78	3.87	3.95	3.81
-33	3.71	3.81	3.89	3.75
-34	3.65	3.74	3.82	3.68
-35	3.59	3.68	3.76	3.62
-36	3.52	3.62	3.70	3.56
-37	3.46	3.55	3.63	3.49
-38	3.40	3.49	3.57	3.43
-39	3.33	3.43	3.51	3.37
-40	3.27	3.36	3.44	3.30
-41	3.21	3.30	3.38	3.24
-42	3.14	3.24	3.32	3.18
-43	3.08	3.17	3.25	3.11
-44	3.02	3.11	3.19	3.05
-45	2.95	3.05	3.13	2.98
-46	2.89	2.98	3.06	2.92
-47	2.83	2.92	3.00	2.86
-48	2.76	2.86	2.94	2.79
-49	2.70	2.79	2.87	2.73
-50	2.64	2.73	2.81	2.67
-51	2.57	2.67	2.75	2.60
-52	2.51	2.60	2.68	2.54

RSL (dBm)	Channel separation 7, 13.75, 14, 27.5, 28, 29.65, 55, 56, 60 or 80 MHz	Bandwidth 10, 20 or 40 MHz	Bandwidth 30 MHz	Bandwidth 50 MHz
-53	2.45	2.54	2.62	2.48
-54	2.38	2.48	2.55	2.41
-55	2.32	2.41	2.49	2.35
-56	2.26	2.35	2.43	2.29
-57	2.19	2.29	2.36	2.22
-58	2.13	2.22	2.30	2.16
-59	2.07	2.16	2.24	2.10
-60	2.00	2.10	2.17	2.03
-61	1.94	2.03	2.11	1.97
-62	1.88	1.97	2.05	1.91
-63	1.81	1.90	1.98	1.84
-64	1.75	1.84	1.92	1.78
-65	1.69	1.78	1.86	1.72
-66	1.62	1.71	1.79	1.65
-67	1.56	1.65	1.73	1.59
-68	1.50	1.59	1.67	1.53
-69	1.43	1.52	1.60	1.46
-70	1.37	1.46	1.54	1.40
-71	1.31	1.40	1.48	1.34
-72	1.24	1.33	1.41	1.27
-73	1.18	1.27	1.35	1.21
-74	1.11	1.21	1.29	1.15
-75	1.05	1.14	1.22	1.08
-76	0.99	1.08	1.16	1.02
-77	0.92	1.02	1.10	0.96
-78	0.86	0.95	1.03	0.89
-79	0.80	0.89	0.97	0.83
-80	0.73	0.83	0.91	0.77

RSL (dBm)	Channel separation 7, 13.75, 14, 27.5, 28, 29.65, 55, 56, 60 or 80 MHz	Bandwidth 10, 20 or 40 MHz	Bandwidth 30 MHz	Bandwidth 50 MHz
-81	0.67	0.76	0.84	0.70
-82	0.61	0.70	0.78	0.64
-83	0.54	0.64	0.72	0.58
-84	0.48	0.57	0.65	0.51
-85	0.42	0.51	0.59	0.45
-86	0.35	0.45	0.53	0.39
-87	0.29	0.38	0.46	0.32
-88	0.23	0.32	0.40	0.26
-89	0.16	0.26	0.34	0.19
-90	0.10	0.19	0.27	0.13

IRFU specifications

The PTP 800 IRFU conforms to the specifications in Table 83, Table 84, Table 85, and Table 86 and Table 87.

Table 83 IRFU physical specifications

Category	Specification
Rack mounting space (RMS)	Less than 3 RMS (2.77 U) in a NEBS standard 19” rack, for an IRFU with 2 transceivers and associated BU.
Dimensions (approx)	W x D x H (mm): 432 x 280 x 123 W x D x H (in): 17 x 11 x 4.843
Weight	8.1 Kg for 1+0 configuration, including the BU. 11.8 Kg for 1+1 MHSB configuration, including the BU.

Table 84 IRFU electrical specifications

Category	Specification
Input voltage	-48 V dc
Power feed for the RFU transceiver	Direct feed by battery
Power supply inrush current	Compliant to ETS 300 132-2

Table 85 IRFU environmental specifications

Category	Specification
Operational temperature range	-5 to +50 °C
Storage	-45 to + 80 °C
Humidity	Up to 95%, non-condensing
Altitude	0 to 5000 m AMSL
Vibration	EN 300 019-2-3, class 3.2
Transit vibration (packaged equipment)	EN 300 019-2-2, class 2.3
Transit shock (packaged equipment)	EN 300 019-2-2, class 2.3
Earthquake	EN 300 019-2-3

Table 86 IRFU EMC and safety compliance

Category	Specification
Radiated and conducted susceptibility	RF Magnetic field: IEC 61000-4-3 Electrical Fast Transient/Burst: IEC 61000-4-4 ESD: IEC 61000-4-2
Radiated emission and conducted emission	CISPR 22, Class B FCC 47 CFR Part 15, subpart B, Class B Canada ICES-003, Class B
Safety requirements	IEC 60950-1 2006, Second Edition

Table 87 IRFU transceiver power consumption

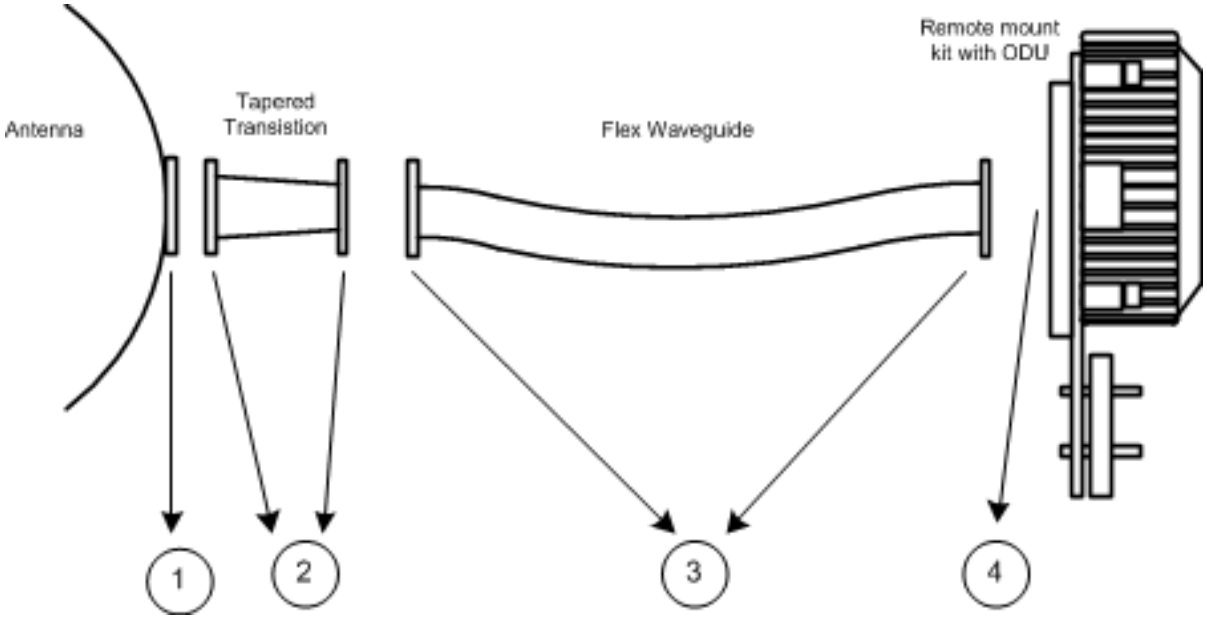
Transceiver type and status	6 GHz Power Consumption @ 48 V (W)	11 GHz Power Consumption @ 48 V (W)
1+0 IRFU transceiver with fans operating	81	71
1+1 Active IRFU transceiver with fans operating	81	71
1+1 Inactive IRFU transceiver with fans off	68.8	60.5

Flexible waveguide specifications

Waveguide flanges

Figure 67 shows the locations of the flanges on the antenna, transition, waveguide and remote mounting kit (RMK). The numbers (1 to 4) refer to Table 88.

Figure 67 Locations of waveguide flanges



The numbered call-outs in Figure 67 are:

1. Antenna flange
2. Tapered transition flanges
3. Flexible waveguide flanges
4. RMK flange

Flanges for each frequency variant

Table 88 specifies the antenna, transition, waveguide and RMK flanges for each frequency variant.

Table 88 Antenna, transition, waveguide and RMK flanges

Frequency	1 Antenna flange	2 Tapered transition flanges	3 Waveguide flange (antenna)	3 Waveguide flange (ODU)	4 RMK flange	Wave guide size
6 GHz (*)	PDR70	n/a	UDR70	PDR70	UDR70	WR137
6 GHz (*)	CPR137G	n/a	CPR137G	PDR70	UDR70	WR137
7 GHz	PDR84	n/a	UDR84	PBR84	UBR84	WR112
8 GHz	PDR84	n/a	UDR84	PBR84	UBR84	WR112
11 GHz	PDR100	UDR100/ PBR120	UBR120	PBR120	UBR120	WR75
13 GHz	PBR120	n/a	UBR120	PBR120	UBR120	WR75
15 GHz	PBR140	n/a	UBR140	PBR140	UBR140	WR62
18 GHz	PBR220	n/a	UBR220	PBR220	UBR220	WR42
23 GHz	PBR220	n/a	UBR220	PBR220	UBR220	WR42
26 GHz	PBR220	n/a	UBR220	PBR220	UBR220	WR42
32 GHz	PBR320	n/a	UBR320	PBR320	UBR320	WR28
38 GHz	PBR320	n/a	UBR320	PBR320	UBR320	WR28

(*) These flanges are used for both Lower 6 GHz and Upper 6 GHz.

Waveguide flange diagrams

Waveguide flanges are illustrated in Figure 68 (Lower and Upper 6 GHz), Figure 69 (7 to 15 GHz), Figure 70 (18 to 38 GHz) and Figure 71 (11 GHz tapered transition).

Figure 68 Waveguide flanges – 6 GHz

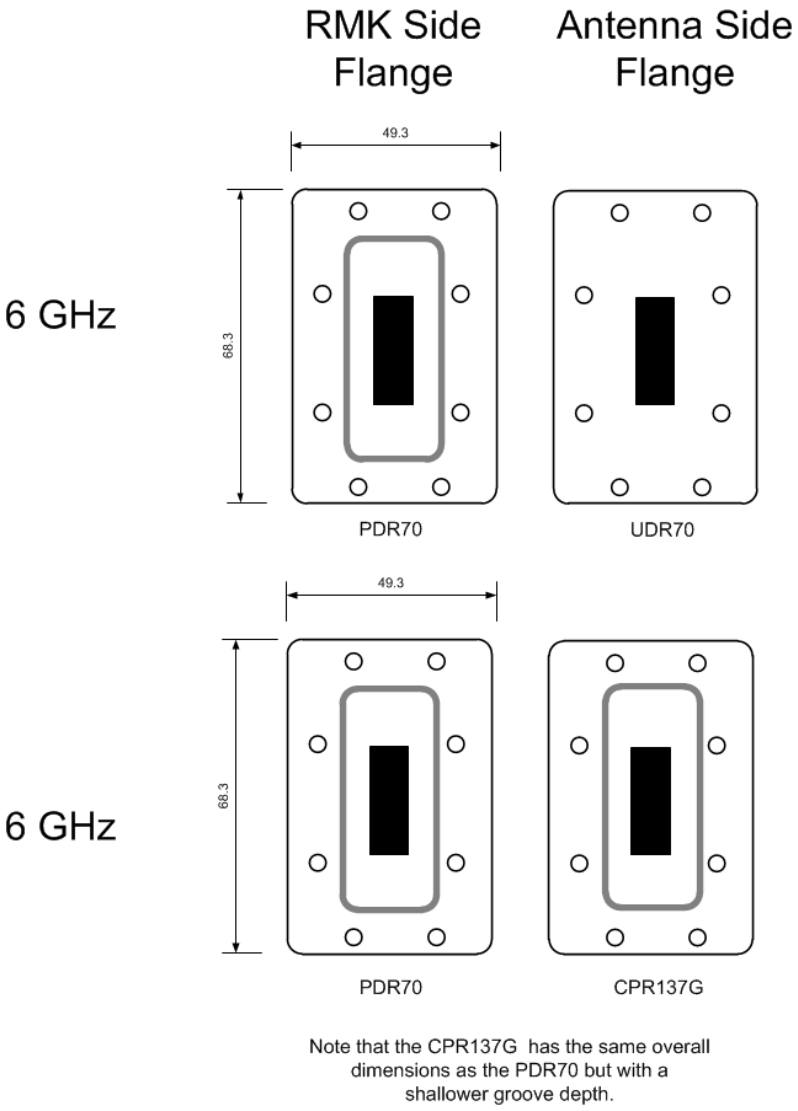


Figure 69 Waveguide flanges – 7 to 15 GHz

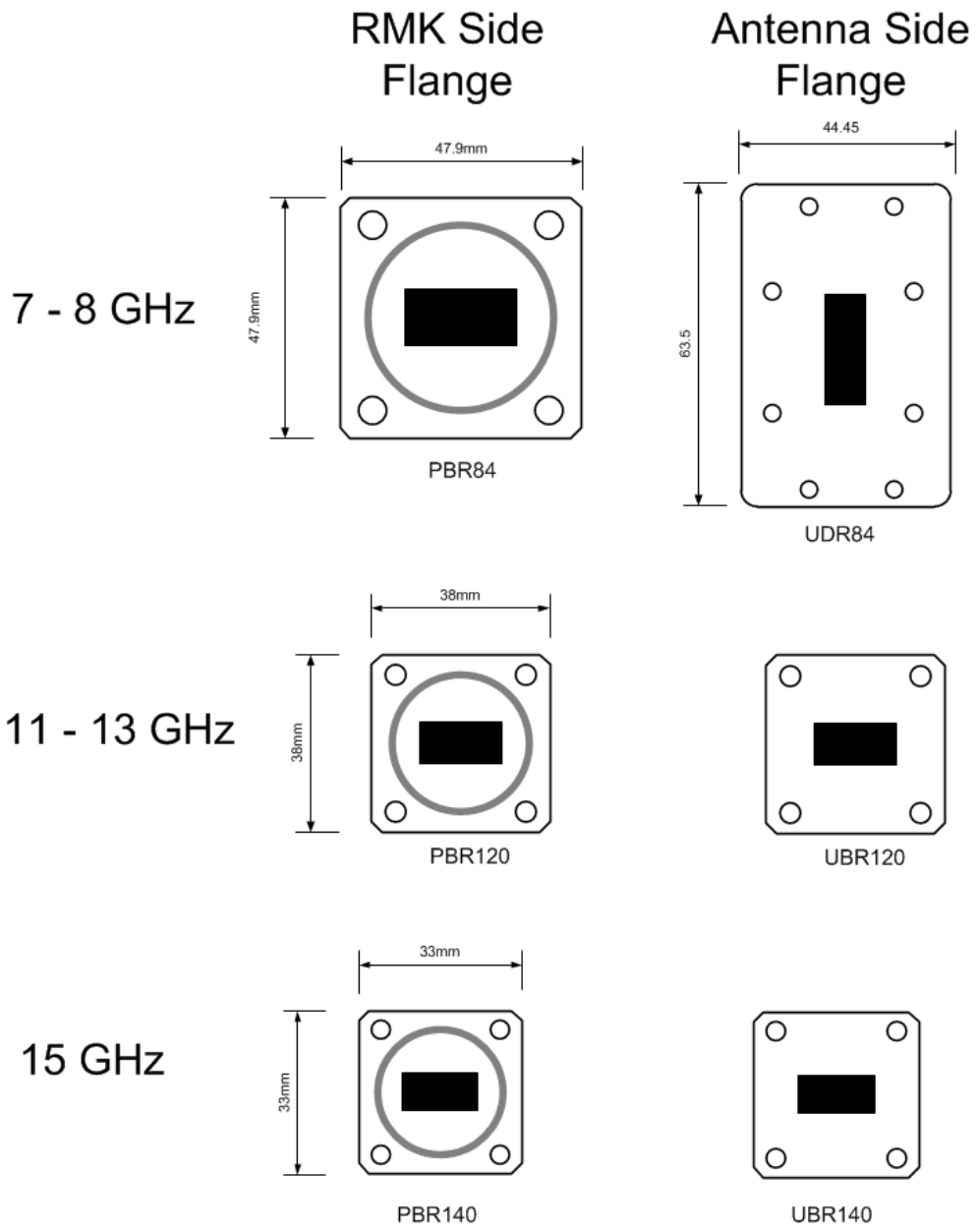


Figure 70 Waveguide flanges – 18 to 38 GHz

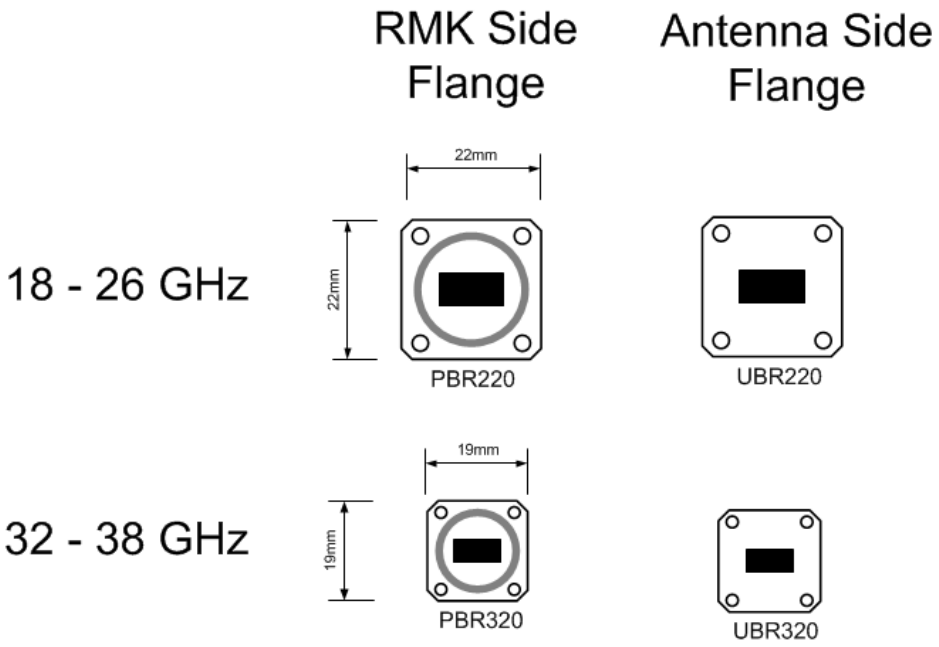
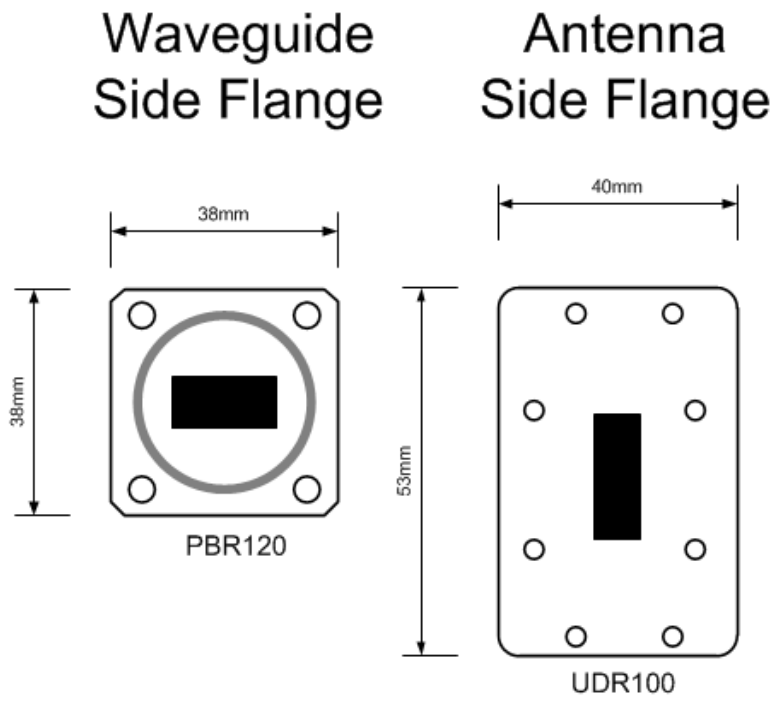


Figure 71 Waveguide flanges – 11 GHz tapered transition



Torque values for waveguide flanges

To obtain the correct torque values for fastening waveguides, refer to Table 89.

Table 89 Torque value in Nm (lb ft) for each fastener size

Material	M3	M4	M5	M6	M8
Stainless steel	0.9 (0.6)	2.2 (1.6)	4.5 (3.3)	7.7 (5.7)	18.7 (13.8)

Coupler mounting kit specifications

The PTP 800 ODU coupler mounting kits conform to the specifications listed in Table 90 and Table 91.

Table 90 ODU coupler physical specifications

Category	Specification
Packed dimensions	250 x 280 x 390 (W x L x H) mm 10 x 11 x 15.5 (W x L x H) ins
Weight	6 GHz band: 7 GHz to 11 GHz bands: 4.6 kg (10.1 lbs) 13 GHz to 38 GHz bands: 4.2 kg (9.3 lbs)

Table 91 ODU coupler environmental specifications

Category	Specification
Temperature	–40°C to 50°C
Relative humidity	0% to 100%
Weatherproofing	IP67
Exposure	Salt mist, industrial atmospheres and UV radiation
Shock and Vibration	ETSI EN 300 019-2-4 (class 4.1E) IEC class 4M5

Coupler losses and isolation

Table 92 contains ODU port return losses and isolation figures for Cambium-supplied ODU couplers. These figures apply to both symmetric and asymmetric couplers.

Table 92 ODU coupler return losses and isolation

Bands	ODU port return loss	Isolation between ODU ports
6 GHz	18 dB minimum	20 dB minimum
7 GHz to 38 GHz	20 dB maximum	20 dB minimum

Table 93 contains ODU port insertion losses for Cambium-supplied ODU couplers.

Table 93 ODU coupler insertion losses

Bands	Coupler type	ODU port maximum insertion losses
6 GHz	3 dB symmetric	
	6 dB asymmetric	Main 1.9 dB, Standby 6.5 dB
7 GHz to 26 GHz	3 dB symmetric	3.8 dB
	6 dB asymmetric	Main 1.8 dB, Standby 7.2 dB
32 GHz to 38 GHz	3 dB symmetric	4.0 dB
	6 dB asymmetric	Main 2.0 dB, Standby 7.4 dB

Protection interface specifications

Out-of-band protection splitter specifications

The out-of-band protection splitter (Cambium part number WB3807) conforms to the specifications in Table 94.

Table 94 Out-of-band protection splitter specifications

Category	Specification
Operating temperature range	–33°C to 55°C
Storage temperature range	-40°C to 60°C
Humidity	90% non-condensing
Compliance	IEC 721, RoHS, WEEE, CMM
Restrictions	For indoor operation only

Protection cable

The maximum length of the protection cable is 2 meters. The wiring must comply with one of the options given in Table 95:

Table 95 Out-of-band protection cable pin outs

Option 1	Option 2 (Gigabit cross over cable)
1 – 1 2 – 2 3 – 3 4 – 7 5 – 8 6 – 6 7 – 4 8 – 5	1 – 3 2 – 6 3 – 1 4 – 7 5 – 8 6 – 2 7 – 4 8 – 5

Fiber-Y kit specifications

The Fiber-Y kit (Cambium part number WB3806) conforms to the specifications listed in Table 96.

Table 96 Fiber-Y kit specifications

Category	Specification
Operating mode	1000-BASE-SX operating in Multi-Mode with a wavelength of 850 nm
Operating temperature range	–33°C to 55°C
Storage temperature range	-40°C to 60°C
Humidity	90% non-condensing
Compliance	RoHS, WEEE, CMM
Restrictions	For indoor operation only

Wireless specifications

This section contains specifications of the PTP 800 wireless interface, including RF bands, channel width and link loss.

General wireless specifications

The PTP 800 conforms to the general wireless specifications listed in Table 97.

Table 97 General wireless specifications

Feature	Specification
Channel separation (ETSI)	7, 13.75, 14, 27.5, 28, 29.65, 30, 40, 55, 56 or 60 MHz.
Channel bandwidth (FCC/IC)	10, 20, 25, 30, 40, 50 or 80 MHz.
Modulation	QPSK, 8PSK, 16QAM, 32QAM, 64QAM, 128QAM and 256QAM. Fixed or adaptive modulation.
Duplex scheme	Frequency division duplex.
Capacity options	Basic capacity is 10 Mbps in each link direction. May be upgraded via software license key to one of the following capacity levels: 20, 30, 40, 50, 100, 150, 200, 300 Mbps, Unlimited.
Latency	Ultra-low latency, <115 us @ 368 Mbps with 64 bytes frame.
Encryption	FIPS-197 128/256 bit AES encryption.
ATPC	Supported in all configurations.

Frequency bands and channel separation

EN 302 217 refers to the relevant ITU-R and CEPT recommendations which are appropriate for operation in ETSI regions. These are summarized in Table 98.

Table 98 ETSI band plan (ODU-A and ODU-B)

Band	Frequency range (GHz)	Channel separation (MHz)	T/R spacing (MHz)	ERC (CEPT/ERC)	ITU-R
Lower 6 GHz	5.9-6.4	29.65	252.04	14-01 An 1	F.383-8
Upper 6 GHz	6.4-7.1	30, 40, 60	340	14-02E	F.384-10
		7, 14	340	-	-
7 GHz	7.1-7.9	7, 14, 28	154, 161, 168, 196, 245	02-06 Annex 1 and 3	F.385-9
8 GHz	7.7 – 8.5	7, 14, 28	119, 126, 208, 266	-	F.386-8 An 2, 3, 5
		29.65	311.32	-	F.386-8 An 6
11 GHz	10.7-11.7	40	490, 530	12-06E	F.387-10
13 GHz	12.75-13.25	7, 14, 28	266	12-02E	F.497-7
15 GHz	14.4-15.35	7, 14, 28, 56	420, 490, 644, 728	T/R 12-07	F.636-3
			315, 322	-	-
18 GHz	17.7-19.7	7, 13.75, 27.5, 55	1010	12-03E	F.595-9
		7	1008	-	F.595-9 An 3
23 GHz	21.2-23.6	7, 14, 28, 56	1008	13-02E An A	F.637-3 An 3, 5
		7, 14, 28	1232	-	F.637-3 An 1
26 GHz	24.5-26.5	7, 14, 28, 56	1008	13-02E An B	F.748-4 An 1
32 GHz	31.8-33.4	7, 14, 28, 56	812	Rec 01(02)	F.1520-2 An 1, 2
38 GHz	37-39.5	7, 14, 28, 56	1260	T/R 12-01	F.749-2 An 1

FCC 101.147 defines the frequency plans for FCC. These are summarized in Table 99 (ODU platforms) and Table 100 (IRFU platforms).

Table 99 FCC and IC band plan (ODU-A and ODU-B)

Band	Frequency range (GHz)	Bandwidth (MHz)	T/R spacing (MHz)	FCC/IC	Reference
Lower 6 GHz	5.9-6.4	10, 30	252.04	FCC, IC	-
Upper 6 GHz	6.5-6.9	10, 30	160, 170	FCC only	-
11 GHz	10.7-11.7	10, 30, 40	490, 500	FCC, IC	Part 101-147 (o) 10-1-08 Edition
18 GHz	17.7-18.7	10, 20, 30, 40, 50 ODU-B: 80	1560	FCC, IC	Part 101-147 (r) 10-1-08 Edition
23 GHz	21.8-23.6	10, 20, 30, 40, 50	1200	FCC, IC	Part 101-147 (s) 10-1-08 Edition
26 GHz	24.2-25.3	10, 20, 40	800	FCC only	Part 101-147 (s) 10-1-08 Edition
38 GHz	38.6-40	10, 50	700	FCC, IC	-

Table 100 FCC and IC band plan (IRFU platforms)

Band	Frequency range (GHz)	Bandwidth (MHz)	T/R spacing (MHz)	FCC/IC	Reference
Lower 6 GHz	5.9-6.4	10, 30	252.04	FCC, IC	FCC Part 101 SRSP 305.9
Upper 6 GHz	6.5-6.9	10, 30	160, 170	FCC	FCC Part 101
7 GHz	6.9-7.1	25	150	FCC	FCC Notice 11-120
11 GHz	10.7-11.7	10, 30, 40	490, 500	FCC	FCC Part 101
11 GHz	10.7-11.7	10, 30, 40	490, 500	IC	SRSP 310.7

The NTIA Red Book defines the frequency plans for NTIA. These are summarized in Table 101.

Table 101 NTIA band plan

Band	Frequency (GHz)	Bandwidth (MHz)	T/R (MHz)
7 GHz	7.10-7.75	10, 20, 30, 40, 50	300
8 GHz	7.75-8.50	10, 20, 30, 40, 50	360

The frequency plan for Brazil is summarized in Table 102.

Table 102 Brazil band plan

Band	Frequency (GHz)	Channel separation (MHz)	T/R (MHz)	ERC (CEPT)	ITU-R
18 GHz	17.7-19.7	13.75, 27.5, 55	1560		F.595-9 An 7

Capacity, transmit power and sensitivity

This section contains tables of wireless performance for PTP 800 links. The tables specify, for each frequency band, region (FCC and ETSI), bandwidth and modulation mode, the following data:

- **F/R mode**: This means ‘Fixed or reference mode’. It indicates whether or not the modulation mode is available as a fixed or reference mode.
- **Cap (Mbps)**: This means ‘Capacity’. It is the maximum sustained aggregate load applied to the data and management Ethernet ports that can be delivered to the remote Ethernet ports without packet discard. This capacity can be achieved with Ethernet Frames which have the highest configured Quality of Service class. Capacity is approximately 1.5% lower for Ethernet Frames with a lower classification. Please refer to Customer network on page 1-42 for an explanation of Ethernet Frame classification.
- **Sens (dBm)**: This means ‘Sensitivity’ It is the typical receive signal level which produces a Frame Error Rate of 5×10^{-4} using 64 octet frames. This is equivalent to a Bit Error Rate of 1×10^{-6} as defined in EN 302 217 Annex F.
- **ACM-o (dBm)**: This means ‘ACM threshold out'. It is the typical signal level at which a given modulation can no longer be supported. When adaptive modulation is enabled and the signal level falls below this level, the modulation with the next lower capacity is automatically selected.
- **ACM-i (dBm)**: This means 'ACM threshold in'. It is the typical signal level required for a given modulation to be automatically selected when adaptive modulation is enabled.

- **Max tx (dBm)**: This means ‘Maximum transmit power’, the maximum value to which the Maximum Transmit Power parameter may be configured. The PTP 800 will not transmit at a level greater than the configured value of Maximum Transmit Power. However if ATPC is enabled, the PTP 800 may transmit at a lower power than the configured value for Maximum Transmit Power.
- **Min tx (dBm)**: This means ‘Minimum transmit power’, the minimum value to which the Maximum Transmit Power parameter may be configured. If ATPC is enabled, the PTP 800 may transmit at a lower power than the configured value for Minimum Transmit Power.

The tables are ordered by frequency band as follows:

- Wireless performance in the Lower 6 GHz band (ODU) on page 4-24
- Wireless performance in the Upper 6 GHz band (ODU) on page 4-26
- Wireless performance in the 6 GHz band (IRFU) on page 4-29
- Wireless performance in the 7 GHz band on page 4-32
- Wireless performance in the 8 GHz band on page 4-33
- Wireless performance in the 11 GHz band (ODU) on page 4-35
- Wireless performance in the 11 GHz band (IRFU) on page 4-39
- Wireless performance in the 13 GHz band on page 4-42
- Wireless performance in the 15 GHz band on page 4-44
- Wireless performance in the 18 GHz band on page 4-46
- Wireless performance in the 23 GHz band on page 4-54
- Wireless performance in the 26 GHz band on page 4-61
- Wireless performance in the 32 GHz band on page 4-66
- Wireless performance in the 38 GHz band on page 4-68

Wireless performance in the Lower 6 GHz band (ODU)

> **NOTE**
> Applies to ODU deployments only.

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the Lower 6 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 103 Lower 6 GHz FCC and Canada with 10 MHz bandwidth

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.83	Yes	50.7	-74.1	-69	-67.5	22	9
64QAM 0.82	Yes	42.2	-77.3	-72.7	-71.4	22	9
32QAM 0.87	Yes	34.7	-79.3	-74.9	-73.6	22	9
16QAM 0.88	Yes	28.2	-82.2	-78.1	-76.8	22	9
8PSK 0.86	Yes	20.8	-84.5	-79.9	-78.6	22	9
QPSK 0.86	Yes	13.8	-88.9	-	-	22	9

Table 104 Lower 6 GHz FCC and Canada with 30 MHz bandwidth

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	177.4	-67.8	-60.1	-57.5	22	9
128QAM 0.82	Yes	155.1	-70.6	-67.3	-66.1	22	9
64QAM 0.87	Yes	135.4	-73	-69.6	-68.3	22	9
32QAM 0.84	Yes	103.6	-76.3	-73.1	-71.9	22	9
16QAM 0.79	Yes	77.9	-80.1	-77.1	-75.9	22	9
8PSK 0.80	Yes	59.1	-82.3	-78.9	-77.6	22	9
QPSK 0.80	Yes	39.4	-85.9	-	-	22	9

Table 105 Lower 6 GHz ETSI with 29.65 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	170.5	-68.1	-61.2	-59.2	22	14
128QAM 0.84	Yes	151.1	-70.9	-67.5	-66.3	24	14
64QAM 0.82	Yes	125.3	-73.9	-70.4	-69.2	24	14
32QAM 0.85	Yes	101.2	-76.4	-73.2	-71.9	28	14
16QAM 0.79	Yes	74.8	-80.3	-77.3	-76.1	28	14
8PSK 0.80	No	56.8	-	-79	-77.8	28	14
QPSK 0.80	Yes	37.8	-86.1	-	-	30	14

Wireless performance in the Upper 6 GHz band (ODU)

NOTE
Applies to ODU deployments only.

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the Upper 6 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 106 Upper 6 GHz FCC with 10 MHz bandwidth

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.83	Yes	50.8	-74.2	-70.3	-68.9	22	9
64QAM 0.83	Yes	42.8	-77.3	-73.6	-72.4	22	9
32QAM 0.84	Yes	33.6	-79.9	-76.5	-75.3	22	9
16QAM 0.91	Yes	29.1	-82.4	-79.2	-78	22	9
8PSK 0.85	Yes	20.4	-85	-81.3	-80.1	22	9
QPSK 0.86	Yes	13.8	-89.9	-	-	22	9

Table 107 Upper 6 GHz FCC with 30 MHz bandwidth

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	177.4	-67.8	-60.1	-57.5	22	9
128QAM 0.82	Yes	155.1	-70.6	-67.3	-66.1	22	9
64QAM 0.87	Yes	135.4	-73	-69.6	-68.3	22	9
32QAM 0.84	Yes	103.6	-76.3	-73.1	-71.9	22	9
16QAM 0.79	Yes	77.9	-80.1	-77.1	-75.9	22	9
8PSK 0.80	Yes	59.1	-82.3	-78.9	-77.6	22	9
QPSK 0.80	Yes	39.4	-85.9	-	-	22	9

Table 108 Upper 6 GHz ETSI with 7 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	34.4	-76.4	-71.7	-70.3	24	14
64QAM 0.82	Yes	30	-78.8	-74.2	-72.9	24	14
32QAM 0.87	Yes	24.6	-80.8	-76.4	-75.2	26	14
16QAM 0.88	Yes	20	-83.7	-79.6	-78.3	28	14
8PSK 0.86	No	14.7	-	-81.4	-80.1	28	14
QPSK 0.88	Yes	10	-90.4	-	-	30	14

Table 109 Upper 6 GHz ETSI with 14 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	71	-73.4	-68.6	-67.2	24	14
64QAM 0.82	Yes	61.8	-75.7	-71.1	-69.8	24	14
32QAM 0.87	Yes	50.7	-77.7	-73.4	-72.1	26	14
16QAM 0.88	Yes	41.3	-80.6	-76.5	-75.3	28	14
8PSK 0.86	No	30.4	-	-78.3	-77	28	14
QPSK 0.86	Yes	20.3	-87.3	-	-	30	14

Table 110 Upper 6 GHz ETSI with 30 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	170.5	-68.1	-61.2	-59.2	22	14
128QAM 0.84	Yes	151.1	-70.9	-67.5	-66.3	24	14
64QAM 0.82	Yes	125.3	-73.9	-70.4	-69.2	24	14
32QAM 0.85	Yes	101.2	-76.4	-73.2	-71.9	26	14
16QAM 0.79	Yes	74.8	-80.3	-77.3	-76.1	28	14
8PSK 0.80	No	56.8	-	-79	-77.8	28	14
QPSK 0.80	Yes	37.8	-86.1	-	-	30	14

Table 111 Upper 6 GHz ETSI with 40 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	No	236.6	-	-59.8	-57.8	22	14
128QAM 0.82	Yes	206.8	-69.4	-66.1	-64.9	24	14
64QAM 0.88	Yes	181.9	-71.8	-68.4	-67.1	24	14
32QAM 0.92	No	150.7	-	-70.7	-69.5	26	14
16QAM 0.79	No	103.8	-	-75.9	-74.7	28	14
8PSK 0.80	No	78.9	-	-77.6	-76.3	28	14
QPSK 0.80	No	52.5	-	-	-	30	14

Table 112 Upper 6 GHz ETSI with 60 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.91	Yes	368.6	-63.2	-58.1	-56.1	22	14
256QAM 0.80	Yes	347.1	-65.1	-58.1	-56.1	22	14
128QAM 0.82	Yes	303.5	-67.8	-64.5	-63.2	24	14
64QAM 0.82	Yes	255.2	-70.8	-67.3	-66.1	24	14
32QAM 0.84	No	202.7	-	-70.2	-68.9	26	14
16QAM 0.79	No	152.4	-	-74.2	-73	28	14
8PSK 0.80	No	115.8	-	-75.9	-74.7	28	14
QPSK 0.80	No	77.1	-	-	-	30	14

Wireless performance in the 6 GHz band (IRFU)

> **NOTE**
> Applies to IRFU deployments only.

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 6 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

> **NOTE**
> The maximum and minimum transmit powers are the powers at the output of an IRFU transceiver and not at the waveguide interface. The power at the waveguide interface depends on the branching unit configuration, which adds additional loss according to Table 116.
>
> The receive sensitivities are at the input to the IRFU transceiver and not at the waveguide interface. The sensitivity at the waveguide interface depends on the branching unit configuration, which adds additional loss according to Table 117.

Table 113 6 GHz FCC and Canada with 10 MHz bandwidth for IRFU

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.76	Yes	55.9	-72.7	-64.7	-62.1	29	10
128QAM 0.83	Yes	50.2	-75	-64.5	-61.7	30	10
64QAM 0.78	Yes	40.5	-79.2	-71.2	-69.9	31	10
32QAM 0.79	Yes	31.1	-81.8	-75.5	-74.3	32	10
16QAM 0.88	Yes	27.9	-83.8	-78.4	-77.2	33	10
8PSK 0.88	Yes	21	-85.6	-80.6	-79.4	33	10
QPSK 0.79	Yes	12.6	-90.9	-	-	34	10

Table 114 6 GHz FCC with 25 MHz bandwidth for IRFU

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.81	Yes	151.4	-69.5	-62.5	-60.4	29	10
128QAM 0.81	Yes	130.5	-72.9	-62.5	-60.4	30	10
64QAM 0.83	Yes	111	-75.5	-69.5	-68.3	31	10
32QAM 0.87	Yes	90.6	-78	-72	-70.7	32	10
16QAM 0.85	Yes	70.8	-81.5	-74.7	-73.5	33	10
8PSK 0.81	Yes	50.8	-83.9	-78.5	-77.2	33	10
QPSK 0.76	Yes	31.8	-87.3	-	-	34	10

Table 115 6 GHz FCC and Canada with 30 MHz bandwidth for IRFU

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	177.4	-68.6	-61.5	-59.4	29	10
128QAM 0.82	Yes	154.7	-71.9	-68.6	-67.3	30	10
64QAM 0.88	Yes	135.9	-74.1	-70.7	-69.4	31	10
32QAM 0.83	Yes	102.6	-77.7	-74.5	-73.3	32	10
16QAM 0.85	Yes	83.3	-80.8	-77.8	-76.6	33	10
8PSK 0.80	Yes	58.9	-83.1	-79.7	-78.4	33	10
QPSK 0.80	Yes	39.3	-86.8	-	-	34	10

Table 116 Transmit branching unit losses for 6 GHz IRFU

IRFU branching configuration	Tx A BU loss	Tx B BU loss
RFU 1plus0	0	
RFU 1plus1 MHSB Equal RFU 1plus1 MHSB Unequal RFU 1plus0 MHSB Ready Equal RFU 1plus0 MHSB Ready Unequal RFU 1plus1 Tx MHSB Rx SD	0.4	
RFU 2plus0	0	0.5

Table 117 Receive branching unit losses for 6 GHz IRFU

IRFU branching configuration	Rx A BU loss	Rx B BU loss
RFU 1plus0	1.0	
RFU 1plus1 MHSB Equal RFU 1plus0 MHSB Ready Equal	4.2	5.1
RFU 1plus1 MHSB Unequal RFU 1plus0 MHSB Ready Unequal	2.3	8.8
RFU 1plus1 Tx MHSB Rx SD	1.0	0.8
RFU 2plus0	1.0	1.5

Wireless performance in the 7 GHz band

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 7 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 118 7 GHz ETSI with 7 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	34.4	-76.4	-71.7	-70.3	24	14
64QAM 0.82	Yes	30	-78.8	-74.2	-72.9	24	14
32QAM 0.87	No	24.6	-	-76.4	-75.2	28	14
16QAM 0.88	Yes	20	-83.7	-79.6	-78.3	28	14
8PSK 0.86	No	14.7	-	-81.4	-80.1	28	14
QPSK 0.88	Yes	10	-90.4	-	-	30	14

Table 119 7 GHz ETSI with 14 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	71	-73.4	-68.6	-67.2	24	14
64QAM 0.82	Yes	61.8	-75.7	-71.1	-69.8	24	14
32QAM 0.87	Yes	50.7	-77.7	-73.4	-72.1	28	14
16QAM 0.88	Yes	41.3	-80.6	-76.5	-75.3	28	14
8PSK 0.86	No	30.4	-	-78.3	-77	28	14
QPSK 0.86	Yes	20.3	-87.3	-	-	30	14

Table 120 7 GHz ETSI with 28 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	170.5	-68.1	-61.2	-59.2	22	14
128QAM 0.84	Yes	151.1	-70.9	-67.5	-66.3	24	14
64QAM 0.82	Yes	125.3	-73.9	-70.4	-69.2	24	14
32QAM 0.85	Yes	101.2	-76.4	-73.2	-71.9	28	14
16QAM 0.79	Yes	74.8	-80.3	-77.3	-76.1	28	14
8PSK 0.80	No	56.8	-	-79	-77.8	28	14
QPSK 0.80	Yes	37.8	-86.1	-	-	30	14

Wireless performance in the 8 GHz band

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 8 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 121 8 GHz ETSI with 7 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	34.4	-76.4	-71.7	-70.3	24	14
64QAM 0.82	Yes	30	-78.8	-74.2	-72.9	24	14
32QAM 0.87	No	24.6	-	-76.4	-75.2	28	14
16QAM 0.88	Yes	20	-83.7	-79.6	-78.3	28	14
8PSK 0.86	No	14.7	-	-81.4	-80.1	28	14
QPSK 0.88	Yes	10	-90.4	-	-	30	14

Table 122 8 GHz ETSI with 14 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	71	-73.4	-68.6	-67.2	24	14
64QAM 0.82	Yes	61.8	-75.7	-71.1	-69.8	24	14
32QAM 0.87	Yes	50.7	-77.7	-73.4	-72.1	28	14
16QAM 0.88	Yes	41.3	-80.6	-76.5	-75.3	28	14
8PSK 0.86	No	30.4	-	-78.3	-77	28	14
QPSK 0.86	Yes	20.3	-87.3	-	-	30	14

Table 123 8 GHz ETSI with 28 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	170.5	-68.1	-61.2	-59.2	22	14
128QAM 0.84	Yes	151.1	-70.9	-67.5	-66.3	24	14
64QAM 0.82	Yes	125.3	-73.9	-70.4	-69.2	24	14
32QAM 0.85	Yes	101.2	-76.4	-73.2	-71.9	28	14
16QAM 0.79	Yes	74.8	-80.3	-77.3	-76.1	28	14
8PSK 0.80	No	56.8	-	-79	-77.8	28	14
QPSK 0.80	Yes	37.8	-86.1	-	-	30	14

Table 124 8 GHz ETSI with 29.65 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	170.5	-68.1	-61.2	-59.2	22	14
128QAM 0.84	Yes	151.1	-70.9	-67.5	-66.3	24	14
64QAM 0.82	Yes	125.3	-73.9	-70.4	-69.2	24	14
32QAM 0.85	Yes	101.2	-76.4	-73.2	-71.9	28	14
16QAM 0.79	Yes	74.8	-80.3	-77.3	-76.1	28	14
8PSK 0.80	No	56.8	-	-79	-77.8	28	14
QPSK 0.80	Yes	37.8	-86.1	-	-	30	14

Wireless performance in the 11 GHz band (ODU)

> **NOTE**
> Applies to ODU deployments only.

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 11 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 125 11 GHz FCC and Canada with 10 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.83	Yes	50.7	-74.6	-69.5	-68	19	6
64QAM 0.82	Yes	42.2	-77.8	-73.2	-71.9	19	6
32QAM 0.87	Yes	34.7	-79.8	-75.4	-74.1	19	6
16QAM 0.88	Yes	28.2	-82.7	-78.6	-77.3	19	6
8PSK 0.86	Yes	20.8	-85	-80.4	-79.1	19	6
QPSK 0.86	Yes	13.8	-89.4	-	-	19	6

Table 126 11 GHz FCC and Canada with 10 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.83	Yes	50.8	-74.7	-70.8	-69.4	20	5
64QAM 0.83	Yes	42.8	-77.8	-74.1	-72.9	20	5
32QAM 0.84	Yes	33.6	-80.4	-77	-75.8	20	5
16QAM 0.91	Yes	29.1	-82.9	-79.7	-78.5	20	5
8PSK 0.85	Yes	20.4	-85.5	-81.8	-80.6	20	5
QPSK 0.86	Yes	13.8	-90.4	-		20	5

Table 127 11 GHz FCC and Canada with 30 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	177.4	-68.5	-61.5	-59.6	19	6
128QAM 0.82	Yes	155.1	-71.2	-67.9	-66.6	19	6
64QAM 0.82	Yes	130.4	-74.2	-70.8	-69.5	19	6
32QAM 0.84	Yes	103.6	-76.8	-73.6	-72.4	19	6
16QAM 0.79	Yes	77.9	-80.6	-77.6	-76.4	19	6
8PSK 0.80	Yes	59.1	-82.8	-79.4	-78.1	19	6
QPSK 0.80	Yes	39.4	-86.4	-	-	19	6

Table 128 11 GHz FCC and Canada with 30 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	177.4	-68.1	-61	-58.9	20	5
128QAM 0.82	Yes	154.7	-71.4	-68.1	-66.8	20	5
64QAM 0.88	Yes	135.9	-73.6	-70.2	-68.9	20	5
32QAM 0.83	Yes	102.6	-77.2	-74	-72.8	20	5
16QAM 0.85	Yes	83.3	-80.3	-77.3	-76.1	20	5
8PSK 0.80	Yes	58.9	-82.6	-79.2	-77.9	20	5
QPSK 0.80	Yes	39.3	-86.3	-	-	20	5

Table 129 11 GHz FCC and Canada with 40 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	236.6	-67.2	-60.3	-58.3	19	6
128QAM 0.82	Yes	206.8	-69.9	-66.6	-65.4	19	6
64QAM 0.88	Yes	181.9	-72.3	-68.9	-67.6	19	6
32QAM 0.92	Yes	150.7	-74.4	-71.2	-70	19	6
16QAM 0.79	Yes	103.8	-79.3	-76.4	-75.2	19	6
8PSK 0.80	Yes	78.9	-81.5	-78.1	-76.8	19	6
QPSK 0.80	Yes	52.5	-85.1	-	-	19	6

Table 130 11 GHz FCC and Canada with 40 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	236.6	-67.1	-60.1	-58.1	20	5
128QAM 0.82	Yes	206.3	-70	-66.7	-65.5	20	5
64QAM 0.87	Yes	180	-72.5	-69.1	-67.8	20	5
32QAM 0.92	Yes	150.4	-74.4	-71.2	-70	20	5
16QAM 0.85	Yes	111.1	-79	-76.1	-74.9	20	5
8PSK 0.80	Yes	78.5	-81.3	-77.9	-76.6	20	5
QPSK 0.80	Yes	52.4	-85.1	-	-	20	5

Table 131 11 GHz ETSI with 40 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	No	236.6	-	-60.3	-58.3	19	11
128QAM 0.82	Yes	206.8	-69.9	-66.6	-65.4	21	11
64QAM 0.88	Yes	181.9	-72.3	-68.9	-67.6	21	11
32QAM 0.92	No	150.7	-	-71.2	-70	26	11
16QAM 0.79	No	103.8	-	-76.4	-75.2	26	11
8PSK 0.80	No	78.9	-	-78.1	-76.8	26	11
QPSK 0.80	No	52.5	-	-	-	28	11

Wireless performance in the 11 GHz band (IRFU)

> **NOTE**
> Applies to IRFU deployments only.

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 11 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

> **NOTE**
> The maximum and minimum transmit powers are the powers at the output of an IRFU transceiver and not at the waveguide interface. The power at the waveguide interface depends on the branching unit configuration, which adds additional loss according to Table 135.
>
> The receive sensitivities are at the input to the IRFU transceiver and not at the waveguide interface. The sensitivity at the waveguide interface depends on the branching unit configuration, which adds additional loss according to Table 136.

Table 132 11 GHz FCC and Canada with 10 MHz bandwidth for IRFU

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.76	Yes	55.9	-72.2	-64.2	-61.6	26	7
128QAM 0.83	Yes	50.2	-74.5	-64	-61.2	27	7
64QAM 0.78	Yes	40.5	-78.7	-70.7	-69.4	28	7
32QAM 0.79	Yes	31.1	-81.3	-75	-73.8	29	7
16QAM 0.88	Yes	27.9	-83.3	-77.9	-76.7	30	7
8PSK 0.88	Yes	21	-85.1	-80.1	-78.9	30	7
QPSK 0.79	Yes	12.6	-90.4	-	-	31	7

Table 133 11 GHz FCC and Canada with 30 MHz bandwidth for IRFU

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	177.4	-68.1	-61	-58.9	26	7
128QAM 0.82	Yes	154.7	-71.4	-68.1	-66.8	27	7
64QAM 0.88	Yes	135.9	-73.6	-70.2	-68.9	28	7
32QAM 0.83	Yes	102.6	-77.2	-74	-72.8	29	7
16QAM 0.85	Yes	83.3	-80.3	-77.3	-76.1	30	7
8PSK 0.80	Yes	58.9	-82.6	-79.2	-77.9	30	7
QPSK 0.80	Yes	39.3	-86.3	-	-	31	7

Table 134 11 GHz FCC and Canada with 40 MHz bandwidth for IRFU

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	236.6	-67.1	-60.1	-58.1	26	7
128QAM 0.82	Yes	206.3	-70	-66.7	-65.5	27	7
64QAM 0.87	Yes	180	-72.5	-69.1	-67.8	28	7
32QAM 0.92	Yes	150.4	-74.4	-71.2	-70	29	7
16QAM 0.85	Yes	111.1	-79	-76.1	-74.9	30	7
8PSK 0.80	Yes	78.5	-81.3	-77.9	-76.6	30	7
QPSK 0.80	Yes	52.4	-85.1	-	-	31	7

Table 135 Transmit branching unit losses for 11 GHz IRFU

IRFU branching configuration	Tx A BU loss	Tx B BU loss
RFU 1plus0	0	
RFU 1plus1 MHSB Equal RFU 1plus1 MHSB Unequal RFU 1plus0 MHSB Ready Equal RFU 1plus0 MHSB Ready Unequal RFU 1plus1 Tx MHSB Rx SD	0.5	
RFU 2plus0	0	0.7

Table 136 Receive branching unit losses for 11 GHz IRFU

IRFU branching configuration	Rx A BU loss	Rx B BU loss
RFU 1plus0	1.5	
RFU 1plus1 MHSB Equal RFU 1plus0 MHSB Ready Equal	4.8	6.0
RFU 1plus1 MHSB Unequal RFU 1plus0 MHSB Ready Unequal	3.2	9.7
RFU 1plus1 Tx MHSB Rx SD	1.5	1.3
RFU 2plus0	1.5	2.2

Wireless performance in the 13 GHz band

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 13 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 137 13 GHz ETSI with 7 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	34.4	-76.9	-72.2	-70.8	18	8
64QAM 0.82	Yes	30	-79.3	-74.7	-73.4	18	8
32QAM 0.87	No	24.6	-	-76.9	-75.7	23	8
16QAM 0.88	Yes	20	-84.2	-80.1	-78.8	23	8
8PSK 0.86	No	14.7	-	-81.9	-80.6	23	8
QPSK 0.88	Yes	10	-90.9	-	-	26	8

Table 138 13 GHz ETSI with 14 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	71	-73.9	-69.1	-67.7	18	8
64QAM 0.82	Yes	61.8	-76.2	-71.6	-70.3	18	8
32QAM 0.87	Yes	50.7	-78.2	-73.9	-72.6	23	8
16QAM 0.88	Yes	41.3	-81.1	-77	-75.8	23	8
8PSK 0.86	No	30.4	-	-78.8	-77.5	23	8
QPSK 0.86	Yes	20.3	-87.8	-	-	26	8

Table 139 13 GHz ETSI with 28 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	170.5	-68.6	-61.7	-59.7	16	8
128QAM 0.84	Yes	151.1	-71.4	-68	-66.8	18	8
64QAM 0.82	Yes	125.3	-74.4	-70.9	-69.7	18	8
32QAM 0.85	Yes	101.2	-76.9	-73.7	-72.4	23	8
16QAM 0.79	Yes	74.8	-80.8	-77.8	-76.6	23	8
8PSK 0.80	No	56.8	-	-79.5	-78.3	23	8
QPSK 0.80	Yes	37.8	-86.6	-	-	26	8

Wireless performance in the 15 GHz band

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 15 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 140 15 GHz ETSI with 7 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	34.4	-76.9	-72.2	-70.8	18	8
64QAM 0.82	Yes	30	-79.3	-74.7	-73.4	18	8
32QAM 0.87	No	24.6	-	-76.9	-75.7	23	8
16QAM 0.88	Yes	20	-84.2	-80.1	-78.8	23	8
8PSK 0.86	No	14.7	-	-81.9	-80.6	23	8
QPSK 0.88	Yes	10	-90.9	-	-	26	8

Table 141 15 GHz ETSI with 14 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	71	-73.9	-69.1	-67.7	18	8
64QAM 0.82	Yes	61.8	-76.2	-71.6	-70.3	18	8
32QAM 0.87	Yes	50.7	-78.2	-73.9	-72.6	23	8
16QAM 0.88	Yes	41.3	-81.1	-77	-75.8	23	8
8PSK 0.86	No	30.4	-	-78.8	-77.5	23	8
QPSK 0.86	Yes	20.3	-87.8	-	-	26	8

Table 142 15 GHz ETSI with 28 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	170.5	-68.6	-61.7	-59.7	16	8
128QAM 0.84	Yes	151.1	-71.4	-68	-66.8	18	8
64QAM 0.82	Yes	125.3	-74.4	-70.9	-69.7	18	8
32QAM 0.85	Yes	101.2	-76.9	-73.7	-72.4	23	8
16QAM 0.79	Yes	74.8	-80.8	-77.8	-76.6	23	8
8PSK 0.80	No	56.8	-	-79.5	-78.3	23	8
QPSK 0.80	Yes	37.8	-86.6	-	-	26	8

Table 143 15 GHz ETSI with 56 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256 QAM 0.91	Yes	368.6	-63.7	-58.6	-56.6	16	8
256 QAM 0.80	Yes	347.1	-65.6	-58.6	-56.6	16	8
128 QAM 0.82	Yes	303.5	-68.3	-65	-63.7	18	8
64 QAM 0.82	Yes	255.2	-71.3	-67.8	-66.6	18	8
32 QAM 0.84	No	202.7	-	-70.7	-69.4	23	8
16 QAM 0.79	Yes	152.4	-77.7	-74.7	-73.5	23	8
8PSK 0.80	No	115.8	-	-76.4	-75.2	23	8
QPSK 0.80	Yes	77.1	-83.5	-	-	26	8

Wireless performance in the 18 GHz band

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 18 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 144 18 GHz FCC and Canada with 10 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.83	Yes	50.7	-74.6	-69.5	-68	17	2
64QAM 0.82	Yes	42.2	-77.8	-73.2	-71.9	17	2
32QAM 0.87	Yes	34.7	-79.8	-75.4	-74.1	22	2
16QAM 0.88	Yes	28.2	-82.7	-78.6	-77.3	22	2
8PSK 0.86	Yes	20.8	-85	-80.4	-79.1	22	2
QPSK 0.86	Yes	13.8	-89.4	-	-	23	2

Table 145 18 GHz FCC and Canada with 10 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.83	Yes	50.8	-74.7	-70.8	-69.4	19	2
64QAM 0.83	Yes	42.8	-77.8	-74.1	-72.9	19	2
32QAM 0.84	Yes	33.6	-80.4	-77	-75.8	23	2
16QAM 0.91	Yes	29.1	-82.9	-79.7	-78.5	23	2
8PSK 0.85	Yes	20.4	-85.5	-81.8	-80.6	23	2
QPSK 0.86	Yes	13.8	-90.4	-	-	24	2

Table 146 18 GHz FCC and Canada with 20 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.76	Yes	113.7	-70.4	-61.8	-58.9	15	2
128QAM 0.83	Yes	102.2	-72.5	-68.7	-67.4	17	2
64QAM 0.81	Yes	84.9	-75.9	-72.1	-70.9	17	2
32QAM 0.84	Yes	67.8	-78.3	-74.8	-73.5	22	2
16QAM 0.91	Yes	58.5	-80.6	-77.3	-76.1	22	2
8PSK 0.83	Yes	40.3	-83.6	-79.8	-78.6	22	2
QPSK 0.88	Yes	28.5	-87.6	-	-	23	2

Table 147 18 GHz FCC and Canada with 20 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.77	Yes	114.4	-70.2	-61.3	-58.1	17	2
128QAM 0.83	Yes	102	-72.7	-69	-67.7	19	2
64QAM 0.83	Yes	85.5	-75.9	-72.1	-70.9	19	2
32QAM 0.85	Yes	68.8	-78.4	-74.9	-73.6	23	2
16QAM 0.91	Yes	58.4	-80.6	-77.3	-76.1	23	2
8PSK 0.83	Yes	40.4	-83.7	-79.9	-78.7	23	2
QPSK 0.84	Yes	27.1	-88	-	-	24	2

Table 148 18 GHz FCC and Canada with 30 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	177.4	-68.5	-61.5	-59.6	15	2
128QAM 0.82	Yes	155.1	-71.2	-67.9	-66.6	17	2
64QAM 0.82	Yes	130.4	-74.2	-70.8	-69.5	17	2
32QAM 0.84	Yes	103.6	-76.8	-73.6	-72.4	22	2
16QAM 0.79	Yes	77.9	-80.6	-77.6	-76.4	22	2
8PSK 0.80	Yes	59.1	-82.8	-79.4	-78.1	22	2
QPSK 0.80	Yes	39.4	-86.4	-	-	23	2

Table 149 18 GHz FCC and Canada with 30 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	177.4	-68.1	-61	-58.9	17	2
128QAM 0.82	Yes	154.7	-71.4	-68.1	-66.8	19	2
64QAM 0.88	Yes	135.9	-73.6	-70.2	-68.9	19	2
32QAM 0.83	Yes	102.6	-77.2	-74	-72.8	23	2
16QAM 0.85	Yes	83.3	-80.3	-77.3	-76.1	23	2
8PSK 0.80	Yes	58.9	-82.6	-79.2	-77.9	23	2
QPSK 0.80	Yes	39.3	-86.3	-	-	24	2

Table 150 18 GHz FCC and Canada with 40 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	236.6	-67.2	-60.3	-58.3	15	2
128QAM 0.82	Yes	206.8	-69.9	-66.6	-65.4	17	2
64QAM 0.88	Yes	181.9	-72.3	-68.9	-67.6	17	2
32QAM 0.92	Yes	150.7	-74.4	-71.2	-70	22	2
16QAM 0.79	Yes	103.8	-79.3	-76.4	-75.2	22	2
8PSK 0.80	Yes	78.9	-81.5	-78.1	-76.8	22	2
QPSK 0.80	Yes	52.5	-85.1	-	-	23	2

Table 151 18 GHz FCC and Canada with 40 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	236.6	-67.1	-60.1	-58.1	17	2
128QAM 0.82	Yes	206.3	-70	-66.7	-65.5	19	2
64QAM 0.87	Yes	180	-72.5	-69.1	-67.8	19	2
32QAM 0.92	Yes	150.4	-74.4	-71.2	-70	23	2
16QAM 0.85	Yes	111.1	-79	-76.1	-74.9	23	2
8PSK 0.80	Yes	78.5	-81.3	-77.9	-76.6	23	2
QPSK 0.80	Yes	52.4	-85.1	-	-	24	2

Table 152 18 GHz FCC and Canada with 50 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.83	Yes	301.7	-65.8	-58.5	-56.3	15	2
128QAM 0.82	Yes	258.6	-69	-65.6	-64.3	17	2
64QAM 0.82	Yes	217.4	-72	-68.5	-67.2	17	2
32QAM 0.87	Yes	178.6	-74.3	-71	-69.8	22	2
16QAM 0.91	Yes	150.5	-76.3	-73.3	-72	22	2
8PSK 0.84	Yes	103.7	-79.6	-76.1	-74.8	22	2
QPSK 0.80	Yes	65.7	-84.2	-	-	23	2

Table 153 18 GHz FCC and Canada with 50 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.83	Yes	302.1	-65.8	-58.5	-56.3	17	2
128QAM 0.82	Yes	257.8	-69.1	-65.7	-64.4	19	2
64QAM 0.82	Yes	216.5	-72.1	-68.6	-67.3	19	2
32QAM 0.87	Yes	178.6	-74.5	-71.2	-70	23	2
16QAM 0.92	Yes	150.8	-76.7	-73.7	-72.4	23	2
8PSK 0.84	Yes	103.7	-79.9	-76.4	-75.1	23	2
QPSK 0.80	Yes	65.7	-83.9	-	-	24	2

Table 154 18 GHz FCC and Canada with 80 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.91	Yes	368.6	-63.7	-58.6	-56.6	17	2
256QAM 0.80	Yes	347.1	-65.6	-58.6	-56.6	17	2
128QAM 0.82	Yes	303.5	-68.3	-65	-63.7	19	2
64QAM 0.82	Yes	255.2	-71.3	-67.8	-66.6	19	2
32QAM 0.83	Yes	201	-74.1	-70.9	-69.6	23	2
16QAM 0.85	Yes	163.9	-77.3	-74.3	-73.1	23	2
8PSK 0.80	Yes	115.8	-79.9	-76.4	-75.2	23	2
QPSK 0.80	Yes	77.1	-83.5	-	-	24	2

Table 155 18 GHz ETSI with 7 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	34.4	-76.9	-72.2	-70.8	17	7
64QAM 0.82	Yes	30	-79.3	-74.7	-73.4	17	7
32QAM 0.87	No	24.6	-	-76.9	-75.7	22	7
16QAM 0.88	Yes	20	-84.2	-80.1	-78.8	22	7
8PSK 0.86	No	14.7	-	-81.9	-80.6	22	7
QPSK 0.88	Yes	10	-90.9	-	-	25.5	7

Table 156 18 GHz ETSI with 13.75 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	69.8	-74	-69.2	-67.8	17	7
64QAM 0.82	Yes	60.7	-76.3	-71.7	-70.4	17	7
32QAM 0.87	Yes	49.9	-78.3	-73.9	-72.7	22	7
16QAM 0.88	Yes	40.6	-81.2	-77.1	-75.8	22	7
8PSK 0.86	No	29.9	-	-78.9	-77.6	22	7
QPSK 0.86	Yes	19.9	-87.9	-	-	25.5	7

Table 157 18 GHz ETSI with 27.5 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	167	-68.7	-61.8	-59.8	15	7
128QAM 0.84	Yes	148	-71.4	-68.1	-66.9	17	7
64QAM 0.82	Yes	122.7	-74.4	-71	-69.8	17	7
32QAM 0.85	Yes	99.1	-76.9	-73.8	-72.5	22	7
16QAM 0.79	Yes	73.3	-80.8	-77.9	-76.7	22	7
8PSK 0.80	No	55.7	-	-79.6	-78.4	22	7
QPSK 0.80	Yes	37	-86.6	-	-	25.5	7

Table 158 18 GHz ETSI with 55 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.91	Yes	364.9	-63.7	-58.6	-56.7	15	7
256QAM 0.80	Yes	343.6	-65.6	-58.6	-56.7	15	7
128QAM 0.82	Yes	300.4	-68.3	-65	-63.8	17	7
64QAM 0.82	Yes	252.6	-71.3	-67.9	-66.6	17	7
32QAM 0.84	No	200.7	-	-70.7	-69.5	22	7
16QAM 0.79	Yes	150.9	-77.7	-74.8	-73.5	22	7
8PSK 0.80	No	114.6	-	-76.5	-75.2	22	7
QPSK 0.80	Yes	76.3	-83.5	-	-	25.5	7

Table 159 18 GHz Brazil with 13.75 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	No	69.8	-	-69.2	-67.8	17	7
64QAM 0.82	No	60.7	-	-71.7	-70.4	17	7
32QAM 0.87	Yes	49.9	-78.3	-73.9	-72.7	22	7
16QAM 0.88	Yes	40.6	-81.2	-77.1	-75.8	22	7
8PSK 0.86	No	29.9	-	-78.9	-77.6	22	7
QPSK 0.86	Yes	19.9	-87.9	-	-	25.5	7

Table 160 18 GHz Brazil with 27.5 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	No	167	-	-61.8	-59.8	15	7
128QAM 0.84	Yes	148	-71.4	-68.1	-66.9	17	7
64QAM 0.82	No	122.7	-	-71	-69.8	17	7
32QAM 0.85	No	99.1	-	-73.8	-72.5	22	7
16QAM 0.79	Yes	73.3	-80.8	-77.9	-76.7	22	7
8PSK 0.80	No	55.7	-	-79.6	-78.4	22	7
QPSK 0.80	Yes	37	-86.6	-	-	25.5	7

Table 161 18 GHz Brazil with 55 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.91	No	364.9	-	-58.6	-56.7	15	7
256QAM 0.80	No	343.6	-	-58.6	-56.7	15	7
128QAM 0.82	No	300.4	-	-65	-63.8	17	7
64QAM 0.82	No	252.6	-	-67.9	-66.6	17	7
32QAM 0.84	No	200.7	-	-70.7	-69.5	22	7
16QAM 0.79	Yes	150.9	-77.7	-74.8	-73.5	22	7
8PSK 0.80	No	114.6	-	-76.5	-75.2	22	7

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
QPSK 0.80	No	76.3	-	-	-	25.5	7

Wireless performance in the 23 GHz band

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 23 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 162 23 GHz FCC and Canada with 10 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.83	Yes	50.7	-74.1	-69	-67.5	17	2
64QAM 0.82	Yes	42.2	-77.3	-72.7	-71.4	17	2
32QAM 0.87	Yes	34.7	-79.3	-74.9	-73.6	22	2
16QAM 0.88	Yes	28.2	-82.2	-78.1	-76.8	22	2
8PSK 0.86	Yes	20.8	-84.5	-79.9	-78.6	22	2
QPSK 0.86	Yes	13.8	-88.9	-	-	23	2

Table 163 23 GHz FCC and Canada with 10 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.83	Yes	50.8	-74.2	-70.3	-68.9	19	2
64QAM 0.83	Yes	42.8	-77.3	-73.6	-72.4	19	2
32QAM 0.84	Yes	33.6	-79.9	-76.5	-75.3	23	2
16QAM 0.91	Yes	29.1	-82.4	-79.2	-78	23	2
8PSK 0.85	Yes	20.4	-85	-81.3	-80.1	23	2
QPSK 0.86	Yes	13.8	-89.9	-	-	23	2

Table 164 23 GHz FCC and Canada with 20 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.76	Yes	113.7	-69.9	-61.3	-58.4	15	2
128QAM 0.83	Yes	102.2	-72	-68.2	-66.9	17	2
64QAM 0.81	Yes	84.9	-75.4	-71.6	-70.4	17	2
32QAM 0.84	Yes	67.8	-77.8	-74.3	-73	22	2
16QAM0.91	Yes	58.5	-80.1	-76.8	-75.6	22	2
8PSK 0.83	Yes	40.3	-83.1	-79.3	-78.1	22	2
QPSK 0.88	Yes	28.5	-87.1	-	-	23	2

Table 165 23 GHz FCC and Canada with 20 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.77	Yes	114.4	-69.7	-60.8	-57.6	17	2
128QAM 0.83	Yes	102	-72.2	-68.5	-67.2	19	2
64QAM 0.83	Yes	85.5	-75.4	-71.6	-70.4	19	2
32QAM 0.85	Yes	68.8	-77.9	-74.4	-73.1	23	2
16QAM 0.91	Yes	58.4	-80.1	-76.8	-75.6	23	2
8PSK 0.83	Yes	40.4	-83.2	-79.4	-78.2	23	2
QPSK 0.84	Yes	27.1	-87.5	-	-	23	2

Table 166 23 GHz FCC and Canada with 30 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	177.4	-68	-61	-59.1	15	2
128QAM 0.82	Yes	155.1	-70.7	-67.4	-66.1	17	2
64QAM 0.82	Yes	130.4	-73.7	-70.3	-69	17	2
32QAM 0.84	Yes	103.6	-76.3	-73.1	-71.9	22	2
16QAM 0.79	Yes	77.9	-80.1	-77.1	-75.9	22	2
8PSK 0.80	Yes	59.1	-82.3	-78.9	-77.6	22	2
QPSK 0.80	Yes	39.4	-85.9	-	-	23	2

Table 167 23 GHz FCC and Canada with 30 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	177.4	-67.6	-60.5	-58.4	17	2
128QAM 0.82	Yes	154.7	-70.9	-67.6	-66.3	19	2
64QAM 0.88	Yes	135.9	-73.1	-69.7	-68.4	19	2
32QAM 0.83	Yes	102.6	-76.7	-73.5	-72.3	23	2
16QAM 0.85	Yes	83.3	-79.8	-76.8	-75.6	23	2
8PSK 0.80	Yes	58.9	-82.1	-78.7	-77.4	23	2
QPSK 0.80	Yes	39.3	-85.8	-	-	23	2

Table 168 23 GHz FCC and Canada with 40 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	236.6	-66.7	-59.8	-57.8	15	2
128QAM 0.82	Yes	206.8	-69.4	-66.1	-64.9	17	2
64QAM 0.88	Yes	181.9	-71.8	-68.4	-67.1	17	2
32QAM 0.92	Yes	150.7	-73.9	-70.7	-69.5	22	2
16QAM 0.79	Yes	103.8	-78.8	-75.9	-74.7	22	2
8PSK 0.80	Yes	78.9	-81	-77.6	-76.3	22	2
QPSK 0.80	Yes	52.5	-84.6	-	-	23	2

Table 169 23 GHz FCC and Canada with 40 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	236.6	-66.6	-59.6	-57.6	17	2
128QAM 0.82	Yes	206.3	-69.5	-66.2	-65	19	2
64QAM 0.87	Yes	180	-72	-68.6	-67.3	19	2
32QAM 0.92	Yes	150.4	-73.9	-70.7	-69.5	23	2
16QAM 0.85	Yes	111.1	-78.5	-75.6	-74.4	23	2
8PSK 0.80	Yes	78.5	-80.8	-77.4	-76.1	23	2
QPSK 0.80	Yes	52.4	-84.6	-	-	23	2

Table 170 23 GHz FCC and Canada with 50 MHz bandwidth (ODU-A)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.83	Yes	301.7	-65.3	-58	-55.8	15	2
128QAM 0.82	Yes	258.6	-68.5	-65.1	-63.8	17	2
64QAM 0.82	Yes	217.4	-71.5	-68	-66.7	17	2
32QAM 0.87	Yes	178.6	-73.8	-70.5	-69.3	22	2
16QAM 0.91	Yes	150.5	-75.8	-72.8	-71.5	22	2
8PSK 0.84	Yes	103.7	-79.1	-75.6	-74.3	22	2
QPSK 0.80	Yes	65.7	-83.7	-	-	23	2

Table 171 23 GHz FCC and Canada with 50 MHz bandwidth (ODU-B)

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.83	Yes	302.1	-65.3	-58	-55.8	17	2
128QAM 0.82	Yes	257.8	-68.6	-65.2	-63.9	19	2
64QAM 0.82	Yes	216.5	-71.6	-68.1	-66.8	19	2
32QAM 0.87	Yes	178.6	-74	-70.7	-69.5	23	2
16QAM 0.92	Yes	150.8	-76.2	-73.2	-71.9	23	2
8PSK 0.84	Yes	103.7	-79.4	-75.9	-74.6	23	2
QPSK 0.80	Yes	65.7	-83.4	-	-	23	2

Table 172 23 GHz ETSI with 7 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	34.4	-76.4	-71.7	-70.3	17	2
64QAM 0.82	Yes	30	-78.8	-74.2	-72.9	17	2
32QAM 0.87	No	24.6	-	-76.4	-75.2	22	2
16QAM 0.88	Yes	20	-83.7	-79.6	-78.3	22	2
8PSK 0.86	No	14.7	-	-81.4	-80.1	22	2
QPSK 0.88	Yes	10	-90.4	-	-	25	2

Table 173 23 GHz ETSI with 14 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	71	-73.4	-68.6	-67.2	17	7
64QAM 0.82	Yes	61.8	-75.7	-71.1	-69.8	17	7
32QAM 0.87	No	50.7	-	-73.4	-72.1	22	7
16QAM 0.88	Yes	41.3	-80.6	-76.5	-75.3	22	7
8PSK 0.86	No	30.4	-	-78.3	-77	22	7
QPSK 0.86	Yes	20.3	-87.3	-	-	25	7

Table 174 23 GHz ETSI with 28 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	170.5	-68.1	-61.2	-59.2	15	7
128QAM 0.84	Yes	151.1	-70.9	-67.5	-66.3	17	7
64QAM 0.82	Yes	125.3	-73.9	-70.4	-69.2	17	7
32QAM 0.85	Yes	101.2	-76.4	-73.2	-71.9	22	7
16QAM 0.79	Yes	74.8	-80.3	-77.3	-76.1	22	7
8PSK 0.80	No	56.8	-	-79	-77.8	22	7
QPSK 0.80	Yes	37.8	-86.1	-	-	25	7

Table 175 23 GHz ETSI with 56 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.91	Yes	368.6	-63.2	-58.1	-56.1	15	7
256QAM 0.80	Yes	347.1	-65.1	-58.1	-56.1	15	7
128QAM 0.82	Yes	303.5	-67.8	-64.5	-63.2	17	7
64QAM 0.82	Yes	255.2	-70.8	-67.3	-66.1	17	7
32QAM 0.84	No	202.7	-	-70.2	-68.9	22	7
16QAM 0.79	Yes	152.4	-77.2	-74.2	-73	22	7
8PSK 0.80	No	115.8	-	-75.9	-74.7	22	7
QPSK 0.80	Yes	77.1	-83	-	-	25	7

Wireless performance in the 26 GHz band

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 26 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 176 26 GHz FCC with 10 MHz bandwidth

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.83	Yes	50.8	-74.8	-70.3	-68.9	17	2
64QAM 0.83	Yes	42.8	-77.8	-73.5	-72.3	17	2
32QAM 0.84	Yes	33.6	-80.4	-76.4	-75.1	22	2
16QAM 0.91	Yes	29.1	-82.9	-79.1	-77.9	22	2
8PSK 0.85	Yes	20.4	-85.5	-81.2	-80	22	2
QPSK 0.86	Yes	13.8	-90.4	-	-	23	2

Table 177 26 GHz FCC with 20 MHz bandwidth

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.76	Yes	113.7	-69.9	-61.3	-58.4	15	2
128QAM 0.83	Yes	102.2	-72	-68.2	-66.9	17	2
64QAM 0.81	Yes	84.9	-75.4	-71.6	-70.4	17	2
32QAM 0.84	Yes	67.8	-77.8	-74.3	-73	22	2
16QAM 0.91	Yes	58.5	-80.1	-76.8	-75.6	22	2
8PSK 0.83	Yes	40.3	-83.1	-79.3	-78.1	22	2
QPSK 0.88	Yes	28.5	-87.1	-	-	23	2

Table 178 26 GHz FCC with 40 MHz bandwidth

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	236.6	-66.7	-59.8	-57.8	15	2
128QAM 0.82	Yes	206.8	-69.4	-66.1	-64.9	17	2
64QAM 0.88	Yes	181.9	-71.8	-68.4	-67.1	17	2
32QAM 0.92	Yes	150.7	-73.9	-70.7	-69.5	22	2
16QAM 0.79	Yes	103.8	-78.8	-75.9	-74.7	22	2
8PSK 0.80	Yes	78.9	-81	-77.6	-76.3	22	2
QPSK 0.80	Yes	52.5	-84.6	-	-	23	2

Table 179 26 GHz ETSI with 7 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	34.4	-76.4	-71.7	-70.3	17	7
64QAM 0.82	Yes	30	-78.8	-74.2	-72.9	17	7
32QAM 0.87	No	24.6	-	-76.4	-75.2	22	7
16QAM 0.88	Yes	20	-83.7	-79.6	-78.3	22	7
8PSK 0.86	No	14.7	-	-81.4	-80.1	22	7
QPSK 0.88	Yes	10	-90.4	-	-	25	7

Table 180 26 GHz ETSI with 14 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	71	-73.4	-68.6	-67.2	17	7
64QAM 0.82	Yes	61.8	-75.7	-71.1	-69.8	17	7
32QAM 0.87	No	50.7	-	-73.4	-72.1	22	7
16QAM 0.88	Yes	41.3	-80.6	-76.5	-75.3	22	7
8PSK 0.86	No	30.4	-	-78.3	-77	22	7
QPSK 0.86	Yes	20.3	-87.3	-	-	25	7

Table 181 26 GHz ETSI with 28 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	170.5	-68.1	-61.2	-59.2	15	7
128QAM 0.84	Yes	151.1	-70.9	-67.5	-66.3	17	7
64QAM 0.82	Yes	125.3	-73.9	-70.4	-69.2	17	7
32QAM 0.85	Yes	101.2	-76.4	-73.2	-71.9	22	7
16QAM 0.79	Yes	74.8	-80.3	-77.3	-76.1	22	7
8PSK 0.80	No	56.8	-	-79	-77.8	22	7
QPSK 0.80	Yes	37.8	-86.1	-	-	25	7

Table 182 26 GHz ETSI with 56 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.91	Yes	368.6	-63.2	-58.1	-56.1	15	7
256QAM 0.80	Yes	347.1	-65.1	-58.1	-56.1	15	7
128QAM 0.82	Yes	303.5	-67.8	-64.5	-63.2	17	7
64QAM 0.82	Yes	255.2	-70.8	-67.3	-66.1	17	7
32QAM 0.84	No	202.7	-	-70.2	-68.9	22	7
16QAM 0.79	Yes	152.4	-77.2	-74.2	-73	22	7
8PSK 0.80	No	115.8	-	-75.9	-74.7	22	7
QPSK 0.80	Yes	77.1	-83	-	-	25	7

Wireless performance in the 28 GHz band

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 28 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 183 28 GHz ETSI with 7 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	34.4	-75.9	-71.2	-69.8	17	7
64QAM 0.82	Yes	30	-78.3	-73.7	-72.4	17	7
32QAM 0.87	No	24.6	-	-75.9	-74.7	20	7
16QAM 0.88	Yes	20	-83.2	-79.1	-77.8	22	7
8PSK 0.86	No	14.7	-	-80.9	-79.6	22	7
QPSK 0.88	Yes	10	-89.9	-	-	25	7

Table 184 28 GHz ETSI with 14 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	71	-72.9	-68.1	-66.7	17	7
64QAM 0.82	Yes	61.8	-75.2	-70.6	-69.3	17	7
32QAM 0.87	No	50.7	-	-72.9	-71.6	20	7
16QAM 0.88	Yes	41.3	-80.1	-76.0	-74.8	22	7
8PSK 0.86	No	30.4	-	-77.8	-76.5	22	7
QPSK 0.86	Yes	20.3	-86.8	-	-	25	7

Table 185 28 GHz ETSI with 28 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	170.5	-67.6	-60.7	-58.7	15	7
128QAM 0.84	Yes	151.1	-70.4	-67	-65.8	17	7
64QAM 0.82	Yes	125.3	-73.4	-69.9	-68.7	17	7
32QAM 0.85	Yes	101.2	-75.9	-72.7	-71.4	20	7
16QAM 0.79	Yes	74.8	-79.8	-76.8	-75.6	22	7
8PSK 0.80	No	56.8	-	-78.5	-77.3	22	7
QPSK 0.80	Yes	37.8	-85.6	-	-	25	7

Table 186 28 GHz ETSI with 56 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.91	Yes	368.6	-62.7	-57.6	-55.6	15	7
256QAM 0.80	Yes	347.1	-64.6	-57.6	-55.6	15	7
128QAM 0.82	Yes	303.5	-67.3	-64	-62.7	17	7
64QAM 0.82	Yes	255.2	-70.3	-66.8	-65.6	17	7
32QAM 0.84	No	202.7	-	-69.7	-68.4	20	7
16QAM 0.79	Yes	152.4	-76.7	-73.7	-72.5	22	7
8PSK 0.80	No	115.8	-	-75.4	-74.2	22	7
QPSK 0.80	Yes	77.1	-82.5	-	-	25	7

Wireless performance in the 32 GHz band

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 32 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 187 32 GHz ETSI with 7 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	34.4	-75.4	-70.7	-69.3	16	6
64QAM 0.82	Yes	30	-77.8	-73.2	-71.9	16	6
32QAM 0.87	Yes	24.6	-79.8	-75.4	-74.2	19	6
16QAM 0.88	Yes	20	-82.7	-78.6	-77.3	21	6
8PSK 0.86	No	14.7	-	-80.4	-79.1	21	6
QPSK 0.88	Yes	10	-89.4	-	-	23	6

Table 188 32 GHz ETSI with 14 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	71	-72.4	-67.6	-66.2	16	6
64QAM 0.82	Yes	61.8	-74.7	-70.1	-68.8	16	6
32QAM 0.87	Yes	50.7	-76.7	-72.4	-71.1	19	6
16QAM 0.88	Yes	41.3	-79.6	-75.5	-74.3	21	6
8PSK 0.86	No	30.4	-	-77.3	-76	21	6
QPSK 0.86	Yes	20.3	-86.3	-	-	23	6

Table 189 32 GHz ETSI with 28 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	170.5	-67.1	-60.2	-58.2	14	6
128QAM 0.84	Yes	151.1	-69.9	-66.5	-65.3	16	6
64QAM 0.82	Yes	125.3	-72.9	-69.4	-68.2	16	6
32QAM 0.85	Yes	101.2	-75.4	-72.2	-70.9	19	6
16QAM 0.79	Yes	74.8	-79.3	-76.3	-75.1	21	6
8PSK 0.80	No	56.8	-	-78	-76.8	21	6
QPSK 0.80	Yes	37.8	-85.1	-	-	23	6

Table 190 32 GHz ETSI with 56 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.91	Yes	368.6	-62.2	-57.1	-55.1	14	6
256QAM 0.80	Yes	347.1	-64.1	-57.1	-55.1	14	6
128QAM 0.82	Yes	303.5	-66.8	-63.5	-62.2	16	6
64QAM 0.82	Yes	255.2	-69.8	-66.3	-65.1	16	6
32QAM 0.84	Yes	202.7	-72.4	-69.2	-67.9	19	6
16QAM 0.79	Yes	152.4	-76.2	-73.2	-72	21	6
8PSK 0.80	No	115.8	-	-74.9	-73.7	21	6
QPSK 0.80	Yes	77.1	-82	-	-	23	6

Wireless performance in the 38 GHz band

The following tables contain capacity, transmit power and sensitivity data for PTP 800 links operating in the 38 GHz band. For column definitions, refer to Capacity, transmit power and sensitivity on page 4-22.

Table 191 38 GHz FCC and Canada with 10 MHz bandwidth

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.83	Yes	50.8	-71.8	-67.3	-65.9	16	1
64QAM 0.83	Yes	42.8	-74.8	-70.5	-69.3	16	1
32QAM 0.84	Yes	33.6	-77.4	-73.4	-72.1	20	1
16QAM 0.91	Yes	29.1	-79.9	-76.1	-74.9	20	1
8PSK 0.85	Yes	20.4	-82.5	-78.2	-77	20	1
QPSK 0.86	Yes	13.8	-87.4	-	-	21	1

Table 192 38 GHz FCC and Canada with 50 MHz bandwidth

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.83	Yes	301.7	-62.3	-55	-52.8	14	1
128QAM 0.82	Yes	258.6	-65.5	-62.1	-60.8	16	1
64QAM 0.82	Yes	217.4	-68.5	-65	-63.7	16	1
32QAM 0.87	Yes	178.6	-70.8	-67.5	-66.3	20	1
16QAM 0.91	Yes	150.5	-72.8	-69.8	-68.5	20	1
8PSK 0.84	Yes	103.7	-76.1	-72.6	-71.3	20	1
QPSK 0.80	Yes	65.7	-80.7	-	-	21	1

Table 193 38 GHz ETSI with 7 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	34.4	-74.4	-69.7	-68.3	16	6
64QAM 0.82	Yes	30	-76.8	-72.2	-70.9	16	6
32QAM 0.87	No	24.6	-	-74.4	-73.2	20	6
16QAM 0.88	Yes	20	-81.7	-77.6	-76.3	20	6
8PSK 0.86	No	14.7	-	-79.4	-78.1	20	6
QPSK 0.88	Yes	10	-88.4	-	-	23	6

Table 194 38 GHz ETSI with 14 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
128QAM 0.76	Yes	71	-71.4	-66.6	-65.2	16	6
64QAM 0.82	Yes	61.8	-73.7	-69.1	-67.8	16	6
32QAM 0.87	No	50.7	-	-71.4	-70.1	20	6
16QAM 0.88	Yes	41.3	-78.6	-74.5	-73.3	20	6
8PSK 0.86	No	30.4	-	-76.3	-75	20	6
QPSK 0.86	Yes	20.3	-85.3	-	-	23	6

Table 195 38 GHz ETSI with 28 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.80	Yes	170.5	-66.1	-59.2	-57.2	14	6
128QAM 0.84	Yes	151.1	-68.9	-65.5	-64.3	16	6
64QAM 0.82	Yes	125.3	-71.9	-68.4	-67.2	16	6
32QAM 0.85	Yes	101.2	-74.4	-71.2	-69.9	20	6
16QAM 0.79	Yes	74.8	-78.3	-75.3	-74.1	20	6
8PSK 0.80	No	56.8	-	-77	-75.8	20	6
QPSK 0.80	Yes	37.8	-84.1	-	-	23	6

Table 196 38 GHz ETSI with 56 MHz channel separation

Modulation mode	F/R mode	Cap (Mbps)	Sens (dBm)	ACM-o (dBm)	ACM-i (dBm)	Max tx (dBm)	Min tx (dBm)
256QAM 0.91	Yes	368.6	-61.2	-56.1	-54.1	14	6
256QAM 0.80	Yes	347.1	-63.1	-56.1	-54.1	14	6
128QAM 0.82	Yes	303.5	-65.8	-62.5	-61.2	16	6
64QAM 0.82	Yes	255.2	-68.8	-65.3	-64.1	16	6
32QAM 0.84	No	202.7	-	-68.2	-66.9	20	6
16QAM 0.79	Yes	152.4	-75.2	-72.2	-71	20	6
8PSK 0.80	No	115.8	-	-73.9	-72.7	20	6
QPSK 0.80	Yes	77.1	-81	-	-	23	6

Data network specifications

This section contains specifications of the PTP 800 Ethernet interface.

Ethernet interfaces

The PTP 800 CMU Ethernet ports conform to the specifications listed in Table 197, Table 198, and Table 199.

Table 197 Copper data port specifications

Feature	Specification
Ethernet Speed	1000 Base-T
Auto-negotiation advertisement options	100 Mbps or 1000 Mbps Full Duplex
Forced configuration options	100 Mbps Full Duplex
Auto MDI / MDIX	Enabled when auto-negotiation enabled
Maximum frame size (bytes)	9600

Table 198 Fiber data port specifications

Feature	Specification
Ethernet Speed	1000 Base-SX or 1000 Base-LX. Requires upgrade kit.
Auto-negotiation advertisement options	1000 Mbps Full Duplex
Forced configuration options	None
Auto MDI / MDIX	Not applicable
Maximum frame size (bytes)	9600

Table 199 Management port specifications

Feature	Specification
Ethernet Speed	100 Base-T
Auto-negotiation advertisement options	100 Mbps or 10 Mbps Full Duplex
Forced configuration options	100 Mbps or 10 Mbps Full Duplex
Auto MDI / MDIX	Enabled when auto-negotiation enabled
Maximum frame size (bytes)	2000

Ethernet bridging

The PTP 800 conforms to the Ethernet bridging specifications listed in Table 200.

Table 200 Ethernet bridging specifications

Feature	Specification
Frame types	Ethernet, IEEE 802.3–2008 C-VLAN, IEEE 802.1Q-2005 S-VLAN, IEEE 802.1ad-2005
Service type	Transparent Ethernet bridging equivalent to Ethernet private line (EPL).
Service classes for bridged traffic	Eight queues
QoS Classification	Layer 2 control protocols: Bridge, GARP/MRP, CFM, R-APS, EAPS. Layer 2 priority, based on the priority code point (PCP) in the outermost VLAN tag. Layer 3 priority, based on IPv4 DSCP, IPv6 DSCP, or MPLS Traffic Class.
Scheduling	Strict priority

Syslog message formats

This section describes the format and content of Syslog messages.

Format of syslog server messages

PTP 800 generates syslog messages in this format:

```
SP = “ ” = %x20
CO = “:” = %x3A
SC = “;” = %x3B
LT = “<” = %x3C
GT = “>” = %x3E
syslog = pri header SP message
pri = LT “1”-“182” GT
header = timestamp SP hostname
timestamp = month SP days SP hours “:” minutes “:” seconds
month = “Jan”|“Feb”|“Mar”|“Apr”|“May”|“Jun”|“Jul”|“Aug”|“Sep”|“Oct”|“Nov”|“Dec”
days = “ 1”-“31”
hours = “00”-“23”
minutes = seconds = “00”-“59”
hostname = “0.0.0.0”-“255.255.255.255”
message = “PTP800” CO SP (configuration | status | event)
configuration = “configuration” SC SP attribute-name SC SP (“Web user”|“SNMP user”|“SNTP”)
SC SP “was=” previous-value SC SP “now=” new-value SC
status = “status” SC SP attribute-name SC SP “was=” previous-value SC SP “now=” new-value SC
event = “event” SC SP identifier SC SP event-message-content SC
```

Configuration and status messages

Configuration and status messages contain all of the relevant attributes.

This is an example of a configuration message:

```
PTP800: configuration; IP Address; Web user; was=10.10.10.10;
now=169.254.1.1;
```

This is an example of a status message:

```
PTP800: status; Data Port Status; was=Down; now=Up;
```

Event messages

Event messages are listed in Table 201. Definition of abbreviations:

SC = ";"

SP = " "

This is an example of an event message:

```
PTP800: event; auth_login; web user=MarkT; from=169.254.1.1; port=80;
connection=HTTP; authentication=local;
```

Table 201 Event messages

Facility	Severity	Identifier	Message content
security(4)	warning(4)	auth_idle	"Web user=" user-name SC SP "from=" IP-address SC SP "port=" port-number SC SP "connection=" ("HTTP" | "HTTPS") SC SP "authentication=" ("local" | "RADIUS") SC
security(4)	info(6)	auth_login	
security(4)	warning(4)	auth_login_failed	
security(4)	warning(4)	auth_login_locked	
security(4)	info(6)	auth_logout	
kernel(0)	warning(4)	cold_start	"PTP wireless bridge has reinitialized, reason=" reset-reason SC
security(4)	warning(4)	License_update	"License Key updated" SC
syslog(5)	warning(4)	log_full	"Syslog local flash log is 90% full" SC
syslog(5)	warning(4)	log_wrap	"Syslog local flash log has wrapped" SC
local6(22)	warning(4)	protection_switch	"Protection switch, reason=" protectionSwitchCause SC
security(4)	info(6)	radius_auth	"RADIUS user=" user-name SC SP "server " ("1" | "2") " at " IP-address SP "succeeded" SC
security(4)	warning(4)	radius_auth_fail	"RADIUS user=" user-name SC SP "server " ("1" | "2") " at " IP-address SP ("failed" | "succeeded" | "failed (no response)") SC
security(4)	alert(1)	resource_low	"Potential DoS attack on packet ingress " ("warning" | "cleared") SC

Facility	Severity	Identifier	Message content
local6(22)	warning(4)	rfu_power_button_pressed	"The IRFU Power button has been pressed"
local6(22)	warning(4)	rfu_switch_firmware_banks	"Switching RFU firmware banks following software upgrade"
security(4)	warning(4)	sec_zeroize	"Critical Security Parameters (CSPs) zeroized" SC
local6(22)	warning(4)	snmpv3_asn1	"ASN.1 parse error" SC
security(4)	warning(4)	snmpv3_auth	"Authentication failure" SC
local6(22)	warning(4)	snmpv3_decryption	"Decryption failure" SC
local6(22)	warning(4)	snmpv3_engine_id	"Unknown engine ID" SC
local6(22)	warning(4)	snmpv3_sec_level	"Unknown security level" SC
kernel(0)	warning(4)	sys_reboot	"System Reboot, reason=" reset-reason SC
security(4)	warning(4)	sys_software _upgrade	"Software upgraded from " software-version " to " software-version SC software-version = "800-" digit digit "-" digit digit ("" | "-FIPS" | "-UCAPL") SC
local6(22)	info(6)	system_counters_reset	"System Counters Reset" SC
local6(22)	info(6)	system_statistics_reset	"System Statistics Reset" SC
local6(22)	warning(4)	telnet_idle	"Telnet user=" user-name SC SP "from=" IP-address SC SP "port=" port-number SC
local6(22)	info(6)	telnet_login	
local6(22)	warning(4)	telnet_login_failed	
local6(22)	info(6)	telnet_logout	
local6(22)	info(6)	tftp_complete	"TFTP software upgrade finished" SC
local6(22)	info(6)	tftp_failure	"TFTP software upgrade failed, reason=" reason SC
local6(22)	info(6)	tftp_start	"TFTP software upgrade started" SC
NTP(12)	warning(4)	time_auth_failed	"SNTP authentication failed at IP-address=" IP-address SC SP "port-number=" port SC

Facility	Severity	Identifier	Message content
NTP(12)	warning(4)	time_conn_failed	"SNTP connection failed at IP-address=" IP-address SC SP "port-number=" port SC SP "reason=" reason SC

Network management specifications

This section lists supported SNMP objects from the standard MIB-II, IF-MIB and Bridge-MIB.

Standard SNMP MIBs

PTP 800 supports the following SNMP objects from the standard MIB-II, IF-MIB and Bridge-MIB:

Table 202 Standard SNMP objects

Object identifier	Object name
.1.3.6.1.2.1.1.1	sysDescr
.1.3.6.1.2.1.1.2	sysObjectID
.1.3.6.1.2.1.1.3	sysUpTime
.1.3.6.1.2.1.1.4	sysContact
.1.3.6.1.2.1.1.5	sysName
.1.3.6.1.2.1.1.6	sysLocation
.1.3.6.1.2.1.1.7	sysServices
.1.3.6.1.2.1.2.1	ifNumber
.1.3.6.1.2.1.2.2.1.1	ifIndex
.1.3.6.1.2.1.2.2.1.2	ifDescr
.1.3.6.1.2.1.2.2.1.3	ifType
.1.3.6.1.2.1.2.2.1.4	ifMtu
.1.3.6.1.2.1.2.2.1.5	ifSpeed
.1.3.6.1.2.1.2.2.1.6	ifPhysAddress
.1.3.6.1.2.1.2.2.1.7	ifAdminStatus
.1.3.6.1.2.1.2.2.1.8	ifOperStatus
.1.3.6.1.2.1.2.2.1.9	ifLastChange
.1.3.6.1.2.1.2.2.1.10	ifInOctets
.1.3.6.1.2.1.2.2.1.11	ifInUcastPkts
.1.3.6.1.2.1.2.2.1.12	ifInNUcastPkts

Object identifier	Object name
.1.3.6.1.2.1.2.2.1.13	ifInDiscards
.1.3.6.1.2.1.2.2.1.14	ifInErrors
.1.3.6.1.2.1.2.2.1.15	ifInUnknownProtos
.1.3.6.1.2.1.2.2.1.16	ifOutOctets
.1.3.6.1.2.1.2.2.1.17	ifOutUcastPkts
.1.3.6.1.2.1.2.2.1.18	ifOutNUcastPkts
.1.3.6.1.2.1.2.2.1.19	ifOutDiscards
.1.3.6.1.2.1.2.2.1.20	ifOutErrors
.1.3.6.1.2.1.2.2.1.21	ifOutQLen
.1.3.6.1.2.1.2.2.1.22	ifSpecific
.1.3.6.1.2.1.31.1.1.1.1	ifName
.1.3.6.1.2.1.31.1.1.1.2	ifInMulticastPkts
.1.3.6.1.2.1.31.1.1.1.3	ifInBroadcastPkts
.1.3.6.1.2.1.31.1.1.1.4	ifOutMulticastPkts
.1.3.6.1.2.1.31.1.1.1.5	ifOutBroadcastPkts
.1.3.6.1.2.1.31.1.1.1.6	ifHCInOctets
.1.3.6.1.2.1.31.1.1.1.7	ifHCInUcastPkts
.1.3.6.1.2.1.31.1.1.1.8	ifHCInMulticastPkts
.1.3.6.1.2.1.31.1.1.1.9	ifHCInBroadcastPkts
.1.3.6.1.2.1.31.1.1.1.10	ifHCOutOctets
.1.3.6.1.2.1.31.1.1.1.11	ifHCOutUcastPkts
.1.3.6.1.2.1.31.1.1.1.12	ifHCOutMulticastPkts
.1.3.6.1.2.1.31.1.1.1.13	ifHCOutBroadcastPkts
.1.3.6.1.2.1.31.1.1.1.14	ifLinkUpDownTrapEnable
.1.3.6.1.2.1.31.1.1.1.15	ifHighSpeed
.1.3.6.1.2.1.31.1.1.1.16	ifPromiscuousMode
.1.3.6.1.2.1.31.1.1.1.17	ifConnectorPresent
.1.3.6.1.2.1.31.1.1.1.18	ifAlias
.1.3.6.1.2.1.31.1.1.1.19	ifCounterDiscontinuityTime
.1.3.6.1.2.1.17.1.1	dot1dBaseBridgeAddress

Object identifier	Object name
.1.3.6.1.2.1.17.1.2	dot1dBaseNumPorts
.1.3.6.1.2.1.17.1.3	dot1dBaseType
.1.3.6.1.2.1.17.4.1.1	dot1dBasePort
.1.3.6.1.2.1.17.4.1.2	dot1dBasePortIfIndex
.1.3.6.1.2.1.17.4.1.3	dot1dBasePortCircuit
.1.3.6.1.2.1.17.4.1.4	dot1dBasePortDelayExceededDiscards
.1.3.6.1.2.1.17.4.1.5	dot1dBasePortMtuExceededDiscards

Interfaces

The standard interface MIB for PTP 800 always reports five interfaces as follows:

Table 203 Identification of interfaces

ifIndex	ifDescr	ifType	ifOperStatus
1	wireless interface	propWirelessP2P(157)	up | down
2	ethernet data interface	ethernetCsmacd(6)	up | down
3	ethernet management interface	ethernetCsmacd(6)	up | down
4	telecom channel A interface	ds1(18)	notPresent
5	telecom channel B interface	ds1(18)	notPresent

NOTE

PTP 800 does not support telecom channels. These interfaces are included for consistency with other Cambium PTP products.

Counters

The tables below demonstrate the relationship between counter objects in the standard MIB and attributes on the Detailed Counters page of the web-based management interface:

Table 204 Counters for the wireless interface

MIB object	Detailed counter in the web-based interface
ifInUcastPkts	WirelessDataRxFrames + WirelessManagementRxFrames
ifInDiscards	Sum of WirelessDataRxFramesDiscardedQ*n*

MIB object	Detailed counter in the web-based interface
ifInErrors	WirelessDataRxFramesCRCError
ifHCInUcastPkts	64-bit version of ifInUcastPkts
ifOutUcastPkts	WirelessDataTxFrames + WirelessManagementTxFrames
ifOutDiscards	Sum of WirelessDataTxFramesDiscardedQ*n*
ifHCOutUcastPkts	64-bit version of ifOutUcastPkts

Table 205 Counters for the data interface

MIB object	Detailed counter in the web-based interface
ifInOctets	EthernetDataRxOctets
ifInUcastPkts	EthernetDataRxFrames – EthernetDataRxBroadcastFrames
ifInNUcastPkts	EthernetDataRxBroadcastFrames
ifInErrors	EthernetDataRxFramesCRCError + EthernetDataRxFramesUndersize + EthernetDataRxFramesOversize
ifInBroadcastPkts	EthernetDataRxBroadcastFrames
ifHCInOctets	64-bit version of ifInOctets
ifHCInUcastPkts	64-bit version of ifInUcastPkts
ifHCInBroadcastPkts	64-bit version of ifInBroadcastPkts
ifOutOctets	EthernetDataTxOctets
ifOutUcastPkts	EthernetDataTxFrames
ifHCOutOctets	64-bit version of ifOutOctets
ifHCOutUcastPkts	64-bit version of ifOutUcastPkts

Table 206 Counters for the management interface

MIB object	Detailed counter in the web-based interface
ifInOctets	EthernetManagementRxOctets
ifInUcastPkts	EthernetManagementRxFrames – EthernetDataManagementRxMulticastFrames – EthernetDataManagementRxBroadcastFrames
ifInNUcastPkts	EthernetManagementRxMulticastFrames + EthernetManagementRxBroadcastFrames

MIB object	Detailed counter in the web-based interface
ifInErrors	EthernetManagementRxFramesCRCError + EthernetManagementRxFramesUndersize + EthernetManagementRxFramesOversize
ifInMulticastPkts	EthernetManagementRxMulticastFrames
ifInBroadcastPkts	EthernetManagementRxBroadcastFrames
ifHCInOctets	64-bit version of ifInOctets
ifHCInUcastPkts	64-bit version of ifInUcastPkts
ifHCInMulticastPkts	64-bit version of ifInMulticastPkts
ifHCInBroadcastPkts	64-bit version of ifInBroadcastPkts
ifOutOctets	EthernetManagementTxOctets
ifOutUcastPkts	EthernetManagementTxFrames – EthernetManagementTxMulticastFrames – EthernetManagementTxBroadcastFrames
ifOutNUcastPkts	EthernetManagementTxMulticastFrames + EthernetManagementTxBroadcastFrames
ifOutMulticastPkts	EthernetManagementTxMulticastFrames
ifOutBroadcastPkts	EthernetManagementTxBroadcastFrames
ifHCOutOctets	64-bit version of ifOutOctets
ifHCOutUcastPkts	64-bit version of ifOutUcastPkts
ifHCOutMulticastPkts	64-bit version of ifOutMulticastPkts
ifHCOutBroadcastPkts	64-bit version of ifOutBroadcastPkts

Notifications

PTP 800 supports the following SNMP notifications (traps) in the standard IF-MIB:

Table 207 Supported standard notifications

Object identifier	Object name
.1.3.6.1.6.3.1.1.5.1	coldStart
.1.3.6.1.6.3.1.1.5.3	linkDown
.1.3.6.1.6.3.1.1.5.4	linkUp
.1.3.6.1.6.3.1.1.5.5	authenticationFailure

Electromagnetic compliance

This section describes how the PTP 800 complies with the regulations that are in force in various countries, and contains notifications made to regulatory bodies for the PTP 800.

Electrical safety compliance

The PTP 800 hardware has been tested for compliance to the electrical safety specifications listed in Table 208.

Table 208 Electrical safety specifications

Region	Specification
USA	UL 60950
Canada	CSA C22.2 No.60950
International	CB certified & certificate to IEC 60950

EMC immunity compliance

The PTP 800 has been tested for compliance to the EMC immunity specifications listed in Table 209. The top level Specification is ETSI 301-489.

Table 209 EMC immunity compliance specifications

Specification	Comment
EN 55082-1 Generic EMC and EMI requirements for Europe	
EN 61000-4-2: 2001 Electro Static Discharge (ESD), Class 2, 8 kV air, 4 kV contact discharge	The levels used for testing were increased to ensure immunity to 15kV air and 8kV contact discharges.
EN 61000-4-3 (2006) Radiated Immunity 3 V/m	
EN 61000-4-4: 2004 (Bursts/Fast Transients), Class 4, 4 kV level (power lines AC & DC)	Equipment was tested with level increased for dc input and signal lines @ 0.5 kV open circuit voltage.
EN 61000-4-5 (2006) Surge Immunity	

Specification	Comment
EN 61000-4-6: 1996 (Injected RF), power line, Class 3 @ 10 V/m	Signal lines, Class 3 @ 3 V RMS un-modulated.

Compliance testing

Changes or modifications not expressly approved by Cambium could void the user's authority to operate the system.

This system has achieved Type Approval in various countries around the world. This means that the system has been tested against various local technical regulations and found to comply.

Safety testing

The PTP 800 system has been tested for compliance with IEC 60950-1:2005 Edition 2.0 and IEC 60950-1:2001 Edition 1.0, with deviations applicable for Australia and New Zealand.

ETSI compliance testing

The PTP 800 system has been tested for compliance to harmonized European standard *EN 302 217.2.2 Digital systems operating in frequency bands where frequency coordination is applied*. This covers the essential requirements of Article 3.2 of the R&TTE directive.

It has also been tested for compliance to the electro-magnetic compatibility standards *EN 301 489-1 V1.8.1* and *EN 301 489-4 V1.4.1*. The limits for radiated and conducted radiations of Class A have been applied.

Compliance to the requirements of the R&TTE directive has been confirmed by a Notified Body.

Canada compliance

The PTP 800 system has been tested for compliance to RSS-GEN and the band specific Technical Requirements documents in the SRSP series. The test results have been scrutinized by a TCB who have issued a Certificate of Conformity.

Notifications

General notification

Where necessary, the end user is responsible for obtaining any national licenses required to operate this product and these must be obtained before using the product in any particular country. Contact the appropriate national administrations for details on the conditions of use for the bands in question and any exceptions that might apply.

In order to reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Effective Isotropic Radiated Power (EIRP) is not more than that permitted for successful communication.

United States and Canada notification

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules and with RSS-GEN of Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

NOTE

A Class A Digital Device is a device that is marketed for use in a commercial, industrial or business environment, exclusive of a device which is marketed for use by the general public or is intended to be used in the home.

European Union notification

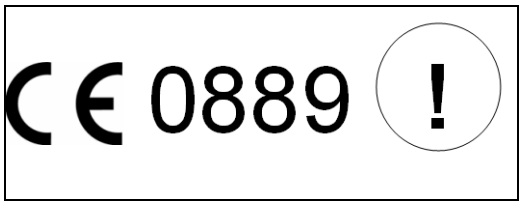
This product complies with the Class A limits for Radiated and Conducted Emissions. It may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce electromagnetic emissions to prevent interference to the reception of radio and television broadcasts.

The PTP 800 is a Class 2 device as it operates on frequencies that are not harmonized across the EU. The operator is responsible for obtaining any national licenses required to operate this product and these must be obtained before using the product in any particular country. See http://www.ero.dk for further information.

Hereby, Cambium Networks declares that the PTP 800 product complies with the essential requirements and other relevant provisions of Directive 1999/5/EC. The declaration of conformity may be consulted at the support web page (see Contacting Cambium Networks on page 2).

This equipment is marked to show compliance with the European R&TTE directive 1999/5/EC.

Figure 72 European Union compliance label



This equipment may be used in the following EU states: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

This equipment may also be used in the following non-EU states that belong to CEPT: Belarus, Iceland, Norway, Switzerland and Turkey.

Thailand notification

เครื่องโทรคมนาคมและอุปกรณ์นี
มีความสอดคล้องตามข้อกำหนดของ กทช.

This telecommunication equipment conforms to the requirements of the National Telecommunications Commission.

Radiation hazard assessment

This section evaluates the radiation levels produced by the PTP 800 products against ETSI and FCC standards.

ETSI method

This section evaluates the radiation levels produced by the PTP 800 products against the following standards:

- *1999/519/EC* of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz).
- *EN 50385:2002* Product standard to demonstrate the compliances of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110 MHz to 40 GHz) — general public.
- *EN 50383:2002* Basic standard for the calculation and measurement of electromagnetic field strength and SAR related to human exposure from radio base stations and fixed terminal stations for wireless telecommunication systems (110 MHz to 40 GHz).

Exposure categories

EN 50385:2002 Clause 3.1 defines the restrictions on exposure to time-varying electric, magnetic, and electromagnetic fields that are based directly on established health effects. Between 10 GHz and 40 GHz, the physical quantity is the power density.

1999/519/EC defines the exposure limit (‘Basic Restriction’) to be considered for the general public. Annex II and Table 1 define this to be 10 W/m^2.

Antenna directivity

The Cambium recommended antennas have Hi-Performance polar patterns in accordance with ETSI EN302 217-4-1 classes 2 and 3. They have gains in excess of 30 dB and beamwidths of less than 5 degrees. Thus, they provide high attenuation of radiated energy at the sides and rear of the antenna.

Calculation

Calculation is used to identify the Compliance Boundary; outside this boundary the radiation levels meet the Basic Restriction, which is defined in *1999/519/EC* as 10 W/m^2.

The distance from the antenna at which the Power Flux Density limit is equal to some specified value is calculated using the Cylindrical Wave model as follows:πð

$$S = \frac{P.180}{\pi D d \delta}$$

Where S = Power density (W/m^2), P = Maximum average transmit power capability of the radio (Watts), D = Antenna diameter (meters), d = Distance from point source (meters), δ = 3 dB antenna beamwidth (degrees).

Rearranging terms to solve for distance yields:

$$d = \frac{P.180}{S \pi D \delta}$$

Distances from antenna

Table 210 specifies calculated minimum separation distances for a range of frequency bands and antenna sizes at the peak of the antenna beam. At these and greater distances, the power density from the RF field is not considered to be hazardous.

Table 210 PTP 800 minimum separation distances, ETSI method

Band	Antenna diameter				
	0.3 m (1 ft)	**0.6 m (2 ft)**	**0.8 m (2.5 ft)**	**1.2 m (4 ft)**	**1.8 m (6 ft)**
6 GHz	N/A	N/A	N/A	1.7 m	1.8 m
7 and 8 GHz	N/A	2.0 m	2.2 m	2.2 m	2.1 m
11 GHz	N/A	1.8 m	2.2 m	2.0 m	1.8 m
13 GHz	1.6 m	1.4 m	1.4 m	1.5 m	1.4 m
15 GHz	1.8 m	1.5 m	1.6 m	1.6 m	1.6 m
18 GHz	2.1 m	1.6 m	1.7 m	1.9 m	1.6 m
23 GHz	2.0 m	1.8 m	2.0 m	2.0 m	2.0 m
26 GHz	2.4 m	2.0 m	2.3 m	2.5 m	N/A
32 and 38 GHz	2.4 m	2.1 m	N/A	N/A	N/A

These separation distances are significantly lower than those calculated by the method specified by the FCC. The ETSI method recognises that radiation is distributed across the antenna aperture and is not in reality a point source.

FCC method

This section evaluates the radiation levels produced by the PTP 800 products against the following standards:

- *ANSI IEEE C95.1-1991, IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz.*
- US FCC limits for the general population. See the FCC web site at http://www.fcc.gov, and the policies, guidelines, and requirements in Part 1 of Title 47 of the *Code of Federal Regulations*, as well as the guidelines and suggestions for evaluating compliance in *FCC OET Bulletin 65*.
- Health Canada limits for the general population. See the Health Canada web site at http://www.hc-sc.gc.ca/ewh-semt/pubs/radiation/99ehd-dhm237/limits-limites_e.html and Safety Code 6.
- ICNIRP (International Commission on Non-Ionizing Radiation Protection) guidelines for the general public. See the ICNIRP web site at http://www.icnirp.de/ and *Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields*.

Calculation

FCC OET Bulletin 65 specifies the far-field method to calculate power density:

$$S = \frac{PG}{4\pi R^2}$$

Where S = Power density (W/m^2), P = Maximum average transmit power capability of the radio (Watts), G = Antenna gain, R = Distance from point source (meters).

FCC Title 47 Part 1.1310 defines the exposure limit for the general population to be 10 W/m^2 (1 mW/cm^2) in the frequency range 1500 to 100,000 MHz. This defines an exposure time of 30 minutes. Higher levels are permitted for shorter periods of exposure.

Rearranging terms to solve for distance yields:

$$R = \sqrt{\frac{4\pi S}{PG}}$$

Distances from antenna

For ODU deployments, Table 211 specifies calculated minimum separation distances for a range of frequency bands and antenna sizes at the peak of the antenna beam. For IRFU deployments, refer to Table 212. At these and greater distances, the power density from the RF field is not considered to be hazardous. These tables are based on the worst case transmit power.

Table 211 PTP 800 minimum separation distances, FCC method (ODU)

Band	Antenna diameter				
	0.3 m (1 ft)	**0.6 m (2 ft)**	**0.8 m (2.5 ft)**	**1.2 m (4 ft)**	**1.8 m (6 ft)**
6 GHz 7 GHz 8 GHz	N/A	N/A	N/A	2.7 m (8.8 ft)	4.2 m (13.6 ft)
11 GHz	N/A	1.9 m (6.3 ft)	2.7 m (8.9 ft)	3.7 m (12.2 ft)	5.6 m (18.4 ft)
18 GHz	2.9 m (9.6 ft)	4.8 m (15.8 ft)	6.3 m (20.7 ft)	9.6 m (31.5 ft)	14.0 m (46.0 ft)
23 GHz	3.0 m (9.9 ft)	5.4 m (17.8 ft)	7.1 m (23.3 ft)	10.7 m (35.2 ft)	14.9 m (48.9 ft)
26 GHz	3.4 m (11.2 ft)	5.9 m (19.4 ft)	8.0 m (26.3 ft)	11.7 m (38.4 ft)	N/A
38 GHz	4.0 m (13.2 ft)	7.4 m (24.3 ft)	N/A	N/A	N/A

Table 212 PTP 800 minimum separation distances, FCC method (IRFU)

Band	Antenna diameter				
	0.3 m (1 ft)	**0.6 m (2 ft)**	**0.8 m (2.5 ft)**	**1.2 m (4 ft)**	**1.8 m (6 ft)**
6 GHz	N/A	N/A	N/A	11.3 m (37.1 ft)	17.4 m (57.1 ft)
11 GHz	N/A	7.1 m (23.3 ft)	10.2 m (33.5 ft)	13.9 m (45.7 ft)	21.0 m (68.9 ft)

Chapter 5: Installation

This chapter describes how to install and test the hardware for a PTP 800 link.

Before starting the installation, refer to:

- Preparing for installation on page 5-2 describes the checks to be performed before proceeding with the installation.

If installing an ODU-based link, refer to:

- Installing antennas and ODUs on page 5-5 describes how to install the antennas, ODUs and waveguide connections at each link end.
- Installing the IF and ground cables on page 5-36 describes how to install the IF cables and how to install grounding and lightning protection.
- Testing the ODU and IF cable on page 5-60 describes how to perform pre-power tests on the ODU, LPUs and IF cable.

If installing or servicing an IRFU-based link, refer to:

- Installing antennas and IRFUs on page 5-70 describes how to install an IRFU with antenna and waveguide.
- Replacing IRFU components on page 5-95 describes how to to replace IRFU components in the field.

To install the CMU and network connections, refer to:

- Installing the CMU on page 5-77 describes how to mount the CMU in the building or cabinet, and to connect it to ground, power supply and PC.
- Preparing network connections (1+0 and 2+0 links) on page 5-84 describes how to prepare the cables to connect the CMU to the customer and (optionally) management networks. It applies only to unprotected ends (1+0 and 2+0 links).
- Preparing network connections (1+1 Hot Standby) on page 5-89 describes how to prepare the cables to connect the CMU to the customer and (optionally) management networks. It applies only to protected ends (1+1 Hot Standby links).

Preparing for installation

Before starting the installation, perform the checks described in this section.

Safety precautions during installation

When developing a site, installing equipment, or performing maintenance, ensure that all national and local safety standards are followed by all personnel.

WARNING

Ensure that personnel are not exposed to unsafe levels of RF energy. The units start to radiate as soon as they are powered up. Respect the safety standards defined in Radiation hazard assessment on page 4-86, in particular the minimum separation distances.

Observe the following guidelines:

- Never work in front of the antenna when the CMU is powered.
- Always power down the CMU before connecting or disconnecting the drop cable from the CMU, ODU or LPU.

Grounding and lightning protection requirements

Ensure that the installation meets the requirements defined in Grounding and lightning protection on page 2-7.

Selecting installation options

Use the installation report to determine which installation options are required. Refer to Link planning on page 2-2.

When installing a 1+1 Hot Standby link, refer to 1+1 Hot Standby link protection on page 1-64 for an overview of alternative hardware configurations.

Preparing personnel

In no event shall Cambium Networks be liable for any injury or damage caused during the installation of the Cambium PTP 800.

Ensure that only qualified personnel undertake the installation of a PTP 800 link.

Ensure that all safety precautions are observed.

Preparing inventory

Perform the following inventory checks:

- Check that an installation report is available and that it is based on the principles described in Chapter 2: Planning considerations.
- Check that the correct components are available, as described Ordering components on page 2-57.
- Check the contents of all packages against their packing lists.

Preparing tools

Check that the tools listed in Table 213 are available.

Table 213 Tools required for PTP 800 installation

Equipment to be Installed	Tools Required
CMU	Pozi screw driver (PZ1) Ground lug crimp tool (diameter 5mm) 8mm spanner
Direct Mount ODU	Lubricant (supplied)
Remote Mount	17mm spanner Lubricant (supplied)
Flexible Wave Guide	Allen key (supplied in the kit)
Flexible Wave Guide hanger	13mm spanner 5mm Allen key Flat bladed screw driver (6mm) or Pozi screw driver (PZ2)

Equipment to be Installed	Tools Required
Coupler	6mm Allen key 2.5mm and 3mm Allen keys (supplied) Lubricant (supplied)
Antenna	17mm spanner 7 mm spanner (for tapered transition) Voltmeter and BNC lead Compass and GPS meter
Cable	Cable cutters Cable hoist Flat file to dress the cable inner core Wire brush to comb the braid Crimp tool Cambium part 66010063001 Torque wrench

Unit pre-configuration

To pre-configure the CMUs during staging before site installation (if this is required), follow this process:

1. Perform the following tasks from Chapter 6: Configuration and alignment for each CMU:

   from Task 1: Connecting to the unit on page 6-3,
   to Task 11: Configuring remote access on page 6-96.

2. Install and test the new hardware by following the relevant procedures in this chapter.

3. Align the antennas and complete the configuration by performing the following tasks from Chapter 6: Configuration and alignment:

   from Task 12: Aligning antennas on page 6-98,
   to Task 15: Connecting link to the network on page 6-114.

Installing antennas and ODUs

NOTE
Applies to ODU deployments only.

This section describes how to install the antennas, ODUs and waveguide connections at each link end.

Use Table 214 to select installation procedures.

Table 214 Selecting antenna and ODU installation procedures

Hardware configuration	Antenna mounting	Antenna protection?	Procedures to be performed
1+0	Direct	-	Installing a direct mount antenna with one ODU on page 5-6.
1+0	Remote	-	Installing a remote mount antenna with one ODU on page 5-9.
1+1	Direct	No	Installing a direct mount antenna with two ODUs (via coupler) on page 5-20.
1+1	Direct	Yes	Installing a direct mount antenna with one ODU on page 5-6. Repeat for the second antenna and ODU.
1+1	Remote	No	Installing a remote mount antenna with two ODUs (via coupler) on page 5-26.
1+1	Remote	Yes	Installing a remote mount antenna with one ODU on page 5-9. Repeat for the second antenna and ODU.
2+0 co-polar	Direct	-	Installing a direct mount antenna with two ODUs (via coupler) on page 5-20.
2+0 co-polar	Remote	-	Installing a remote mount antenna with two ODUs (via coupler) on page 5-26.
2+0 cross-polar	Direct	-	Installing a direct mount dual-polar antenna with two ODUs on page 5-33.
2+0 cross-polar	Remote	-	Installing a remote mount antenna with one ODU on page 5-9. Install two ODUs and waveguides and one dual-polar antenna, but connect both ODUs to the antenna via the waveguide ports.

WARNING

Follow applicable health and safety rules for use of silicone grease. If necessary use the latex gloves supplied with the products.

WARNING

If upgrading an unprotected link to 1+1 Hot Standby, mute the active unit before installing the coupler. For safety reasons this is required when working with the ODUs or when working close to the antenna. See Disabling and enabling the wireless interface on page 7-32.

NOTE

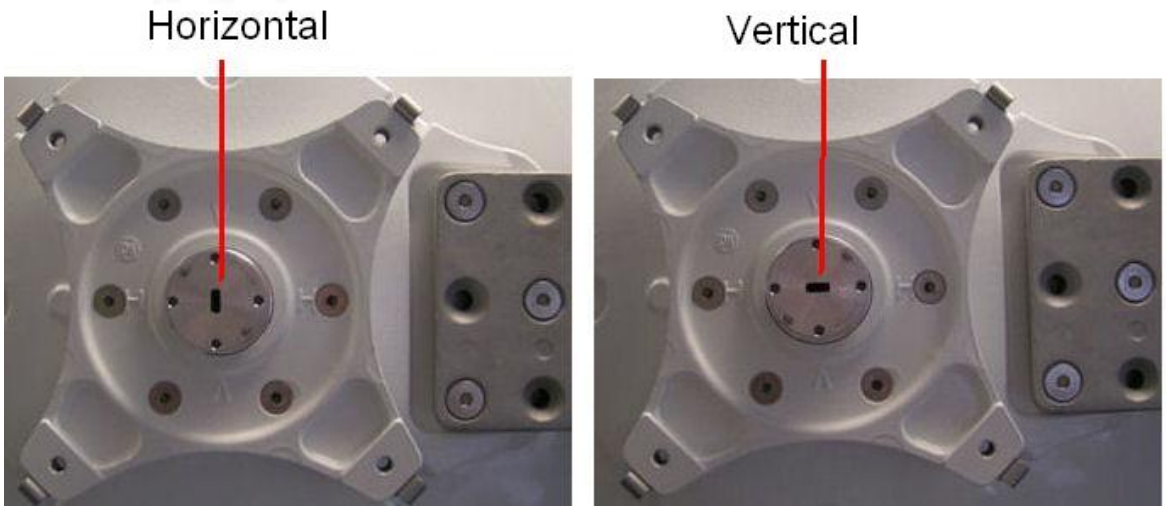
When installing 1+1 Hot Standby links, observe that the ODUs are labeled ‘Hi’ or ‘Lo’ depending on the frequency sub-band. Install the two ‘Hi’ ODUs at one end of the link and the two ‘Lo’ ODUs at the other end.

Installing a direct mount antenna with one ODU

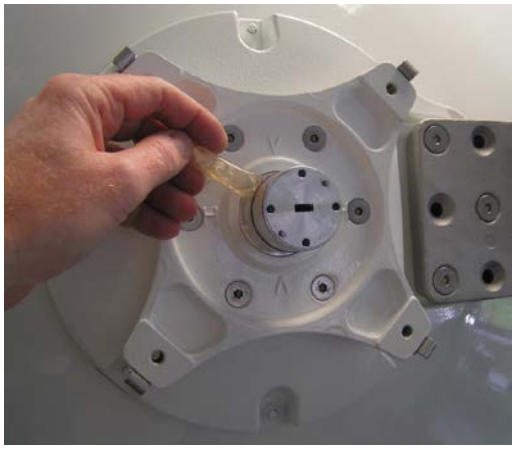
In the direct mount configuration, attach the ODU directly to the antenna (with Cambium ODU interface) via four latches.

To install a direct mount antenna with a single ODU, proceed as follows:

1. Follow the antenna manufacturer’s instructions to attach the antenna to its bracket.
2. Polarization depends upon the antenna waveguide interface position. To change polarization, rotate the antenna transition, following the antenna manufacturer’s instructions.



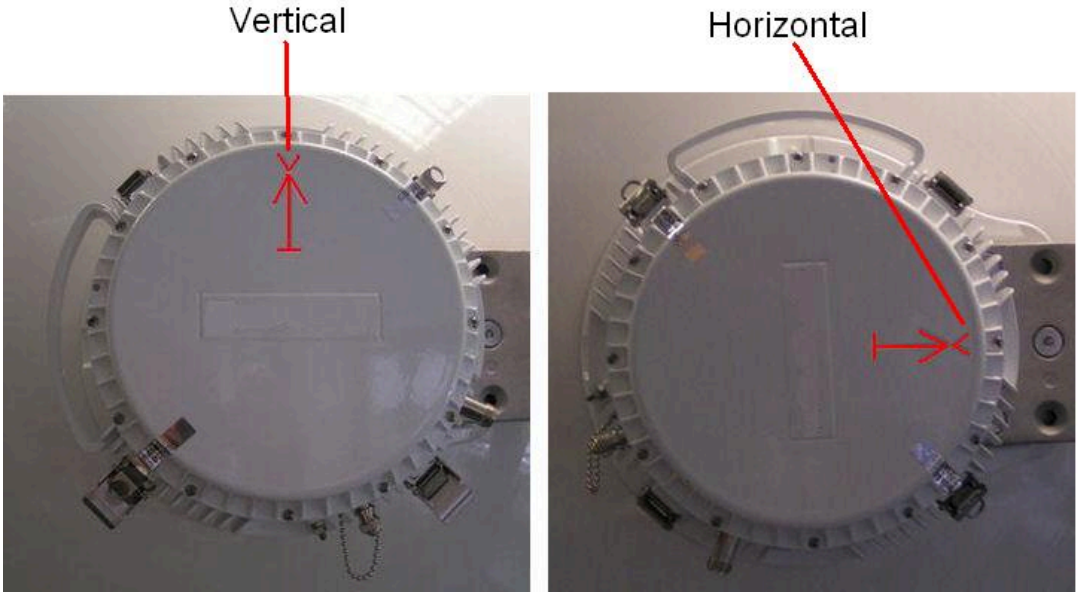
3 Apply silicone grease to the ‘O’ Ring of the antenna transition.



4 Remove the ODU waveguide interface dust cover.



5 Fit the ODU to the antenna transition, ensuring that the antenna and ODU waveguide interfaces align correctly. Observe the polarization of the antenna waveguide interface.



6 Secure the ODU to the antenna with the four latches, taking care to ensure they are correctly engaged.



7 Check that the antenna, mounting bracket and ODU are assembled.



8 Follow the manufacturer's instructions to attach the assembly to the mast or pole.



Installing a remote mount antenna with one ODU

In the remote mount configuration, attach the antenna and ODU to the mast separately, connected to each other via a flexible waveguide. The flexible waveguide is designed to isolate vibration and eliminate difficulties caused by misalignment.

CAUTION

Protect the flexible waveguide from damage that may be caused by contamination, vibration or bending.

When installing a flexible waveguide, observe the following precautions:

- **Unpacking**: To avoid damage to the waveguide, do not unpack it until required. When unpacked, protect the waveguide from dirt, dust or ingress of foreign objects.
- **Vibration:** Flexible waveguides may be damaged if subjected to excessive vibration or excessive bending. If a flexible waveguide is installed in a stressed (tensile) condition, keep vibration to a minimum, as the waveguide rubber jacket may become more susceptible to ozone and general environmental attack. Always use the waveguide hangers; two hangers should be used for the 900mm (3ft) flexible waveguide.
- **Bend radius:** Conform to the bend radii, maximum twist and torque settings specified in Flexible waveguide specifications on page 4-10.
- **Static bend radius:** When installing a flexible waveguide, pay attention to the static bend radius (quoted in the waveguide manufacturer's data sheet). Static bend radius is the minimum bend that an assembly may be subject to without repeat movement (except as a consequence of small vibrations or axial expansions).

NOTE

Before installation, check that the ODU, RMK, waveguide and antenna have compatible interfaces.

NOTE

For a 2+0 cross-polar remote mount configuration, follow the procedures in this section to install two ODUs and waveguides and one dual-polar antenna, but connect both ODUs to the antenna via the waveguide ports (Figure 73).

Figure 73 Dual-polar antenna in remote mount configuration



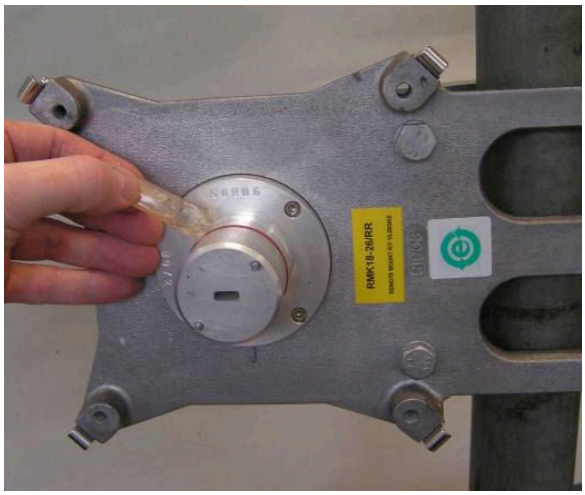
Mounting ODU on pole using RMK

To mount the ODU on the pole using a remote mounting kit (RMK), proceed as follows:

1. Follow the manufacturer's instructions to attach the RMK to the mast or pole.



2. Apply silicone grease to the 'O' ring of the RMK transition.



3. Remove the ODU waveguide interface dust cover.



4 Fit the ODU to the RMK transition, ensuring that the locating pegs on the RMK transition fit into the peg holes in the ODU waveguide interface.



5 Secure the ODU to the RMK with the four latches, taking care to ensure they are correctly engaged.



6 Check that the RMK and ODU are correctly mounted on the mast or pole.



Assembling the flexible waveguide hangers

To provide adequate support for a 900mm flexible waveguide, install two hangers. To assemble the flexible waveguide hangers, proceed as follows:

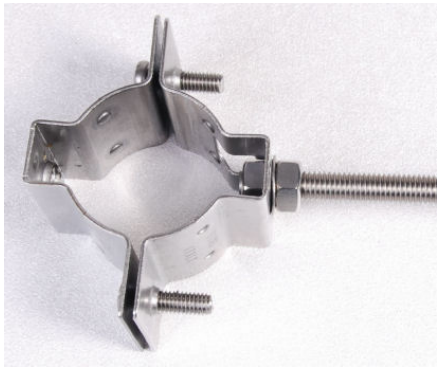
1 Check the flexible waveguide hanger kit contents.



2 Assemble the pole clip, making note of the angle of the slots in the metal strip.



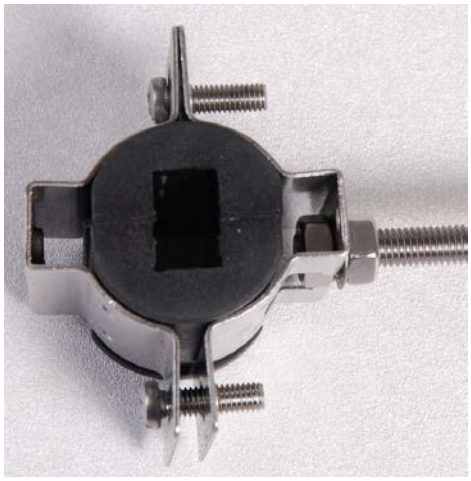
3 Fit the rubber moulding clamp to the studding.



4 Use the 5mm Allen key to fit the pole clip to the studding.



5 Temporarily fit the rubber mouldings.



6 Check the finished assembly.



Attaching antenna and waveguide to pole

> **NOTE**
> If the antenna is 11 GHz, fit a tapered transition between the antenna and waveguide as described in Mounting an 11 GHz antenna with tapered transition and waveguide on page 5-18.

To mount the antenna on the pole and attach it to the ODU via the flexible waveguide, proceed as follows:

1. Follow the antenna manufacturer's instructions to attach the antenna to its bracket and to the mast or pole.
2. Check that the waveguide, antenna and RMK have compatible interfaces. Check that the mating surfaces are clean and free from damage.



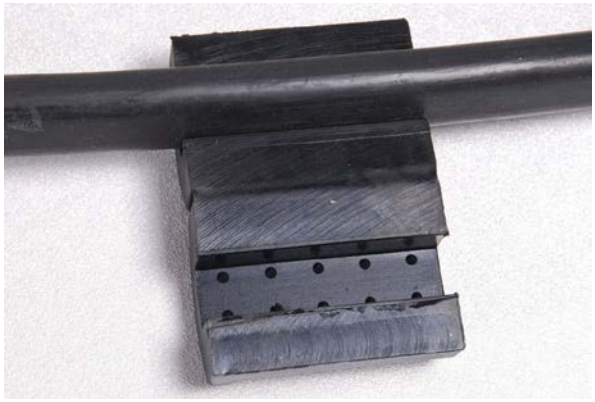
3. Fit one of the 'O' ring seals supplied with the waveguide kit to the flexible waveguide flange that has the O ring groove.
4. Using the waveguide flange fitted with the 'O' ring, fit the flexible waveguide to the remote mount. Ensure that the waveguide cavity orientation matches the opening in the RMK. Fit four shorter screws, using a spring washer and a plain washer on each screw. It is sometimes more convenient to complete this operation before the assembly is fitted to the mast, connecting the flexible waveguide to the antenna when fitting the remote mount to the mast.



5 Fit the remote mount to the tower. Fit an 'O' ring seal to the antenna interface and secure the plain flange of flexible waveguide to the antenna. Ensure that the waveguide cavity orientation matches the opening in the antenna. Secure the flexible waveguide using four of the shorter screws to the antenna. Fit each screw with a spring washer and a plain washer.



6 Fit the rubber inserts from the hanger kit to the flex waveguide.



7 Insert the rubber insert and flex waveguide into the hanger.



8 Fit the hanger cover and tighten.



9 When routing the flex waveguide ensure that the minimum bend radius is not exceeded.



10 Check the complete assembly.



Mounting an 11 GHz antenna with tapered transition and waveguide

When installing an 11 GHz remote mount antenna, fit a tapered transition between the antenna and the flexible waveguide. The tapered transition converts from the PDR100 waveguide flange on the antenna to the UBR120 flange on the flexible waveguide.

To mount an 11 GHz antenna with taper transition and flexible waveguide, proceed as follows:

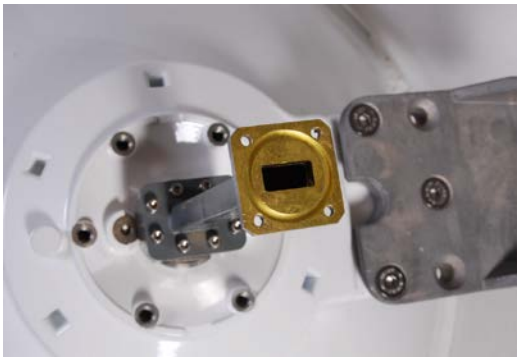
1 Mount the bracket on the antenna.



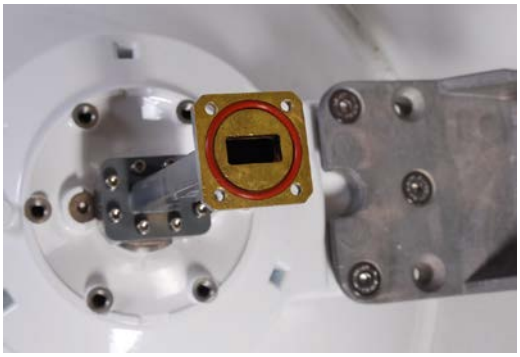
2 Remove the protective film from the antenna waveguide and fit the gasket, (supplied in the kit).



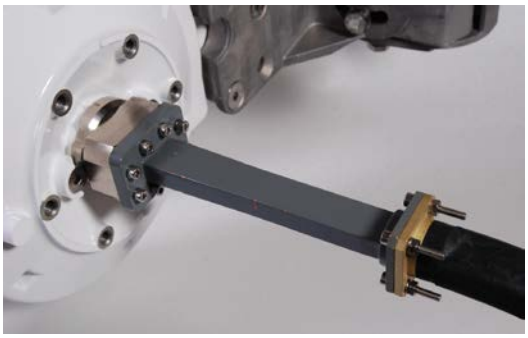
3 Use the 8 screws to fit the tapered transition to the antenna.



4 Fit the seal to the tapered transition, (supplied in the kit).



5 Use the four screws supplied in the kit to fit the flexible waveguide to the tapered transition. It makes taping the joint easier if the four screws are inserted in the direction shown.



6 Use FT-TB fusion tape (Andrews part FT-TB) to water proof the junctions as shown.



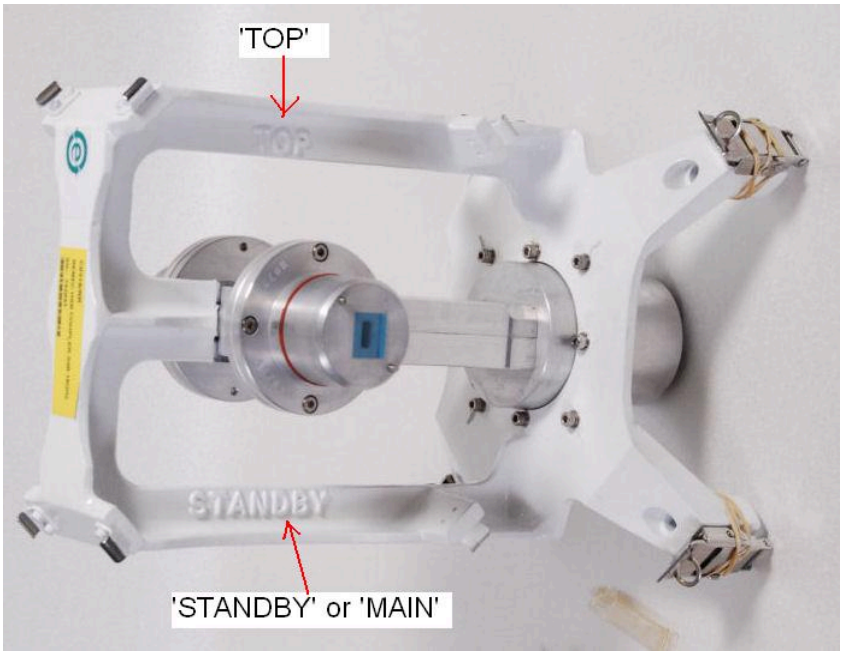
Installing a direct mount antenna with two ODUs (via coupler)

In the direct mount configuration, attach the coupler (with ODUs) directly to the antenna (with Cambium ODU interface) via four latches.

NOTE

If the coupler is asymmetric, one side is embossed with the word ‘MAIN’ and the other side with ‘STANDBY’ (Figure 74). The ‘MAIN’ side has lower loss. Ensure that the ‘MAIN’ and ‘STANDBY’ sides can still be identified after the ODUs are fitted, as this allows them to be connected to the correct CMUs.

Figure 74 Words embossed on coupler (asymmetric shown)



Attaching coupler to antenna

To attach the coupler to the antenna, proceed as follows:

1. Follow the antenna manufacturer's instructions to attach the antenna to its bracket.
2. Check that the supplied coupler is the correct type for this installation. Check the contents of the coupler mounting kit.



3 Fit the correct spacers to each of the four legs:

11GHz - spacer length 27mm

18 GHz, 23 GHz, and 26 GHz - spacer length 7.75mm.



4 For a 1+1 Hot Standby link, check that the circular transitions on the coupler have the same alignment (vertical or horizontal depending on the antenna polarity).

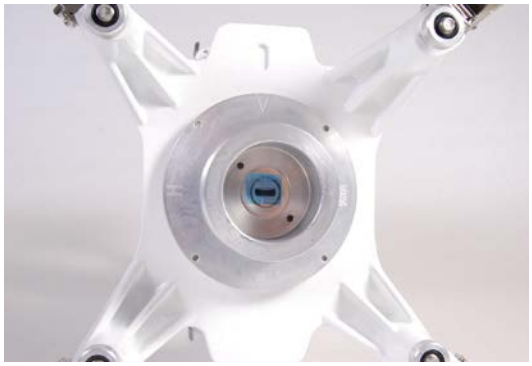
If necessary, rotate the circular transitions according to the manufacturer's instructions.



5 Take note of the word 'TOP' embossed in the casting; ensure this edge is upper most when attached to the antenna.



6 Remove protective film from coupler antenna port.



7 Apply silicone grease to the ‘O’ Ring of the antenna transition.



8 Fit the coupler to the antenna by following this sequence:

Initially, hand-tighten two of the diagonally opposed M8 bolts with the Allen key supplied in the kit.

Using the latch clamp, clip the same two corners.

Repeat the above on the remaining two diagonally opposed bolts and clips.

Torque down all four M8 bolts to 18 Nm.



Attaching ODUs to coupler

To attach the ODUs to the coupler and mount the assembly on the pole, proceed as follows:

1. Remove protective film from the coupler ports.



2. Apply silicone grease to the ‘O’ rings of the coupler transitions.
3. Fit the ODUs to the coupler transitions, ensuring that the waveguide interfaces align correctly for vertical or horizontal polarization. Fit both ODUs such that handles are at the top and connectors at the bottom. For asymmetric couplers, check that the ‘MAIN’ and ‘STANDBY’ sides of the coupler can still be identified.



4 Follow the manufacturer's instructions to attach the assembly to the mast or pole.



5 Check the finished installation.



Installing a remote mount antenna with two ODUs (via coupler)

In the remote mount configuration, attach the antenna and coupler (with two ODUs) to the mast separately, connected to each other via a flexible waveguide. The flexible waveguide is designed to isolate vibration and eliminate difficulties caused by misalignment.

CAUTION

Protect the flexible waveguide from damage that may be caused by contamination, vibration or bending. Observe the precautions in Installing a remote mount antenna with one ODU on page 5-9.

NOTE

Before installation, check that the ODUs, coupler, RMK, waveguide and antenna have compatible interfaces.

NOTE

If the coupler is asymmetric, one side is embossed with the word ‘MAIN’ and the other side with ‘STANDBY’ (Figure 74). The ‘MAIN’ side has lower loss. Ensure that the ‘MAIN’ and ‘STANDBY’ sides can still be identified after the ODUs are fitted, as this allows them to be connected to the correct CMUs.

Attaching coupler to RMK

To attach the coupler to the RMK, proceed as follows:

1 Ensure the correct RMK, coupler and flexible wave guide are present for the frequency band.



2 Check that the supplied coupler is the correct type for this installation. Check the contents of the coupler mounting kit.



3 Fit the correct spacers to each of the four legs:

11GHz - spacer length 27mm

18 GHz, 23 GHz and 26 GHz - spacer length 7.75mm



4 Check that the circular transition on the coupler is correctly aligned for remote mount bracket polarity (vertical or horizontal). If necessary, rotate the circular transition according to the manufacturer's instructions.



5 Take note of the polarization marks on the remote mount bracket.



6 Take note of the word 'TOP' embossed in the casting; ensure this edge is upper most when attached to the antenna.



7 Remove the protective film from the coupler remote mount port.



8 Apply silicone grease to the ‘O’ ring of the remote mount transition.



9 Fit the coupler to the remote mount bracket by following this sequence:

Initially, hand tighten two of the diagonally opposed M8 bolts with the Allen Key supplied in the kit.

Using the latch clamp, clip the same two corners.

Repeat the above on the remaining two diagonally opposed bolts and clips.

Torque down all four M8 bolts to 18Nm.



Assembling the flexible waveguide hangers (remote)

Assemble the hangers as described in Assembling the flexible waveguide hangers on page 5-13.

Attaching antenna to pole

Follow the antenna manufacturer's instructions to attach the antenna to its bracket and to the mast or pole.

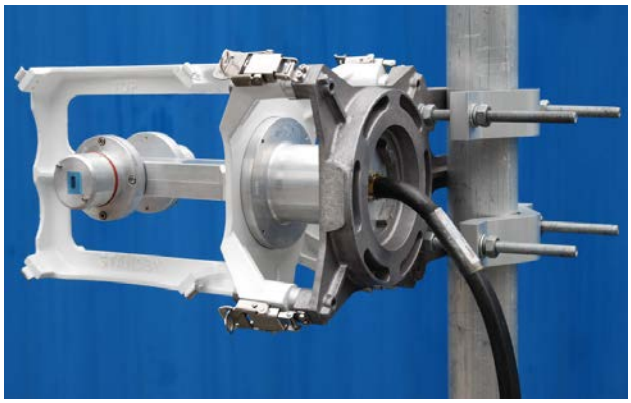
Attaching ODUs to coupler (remote)

To attach the ODUs to the coupler and mount the assembly on the pole, proceed as follows:

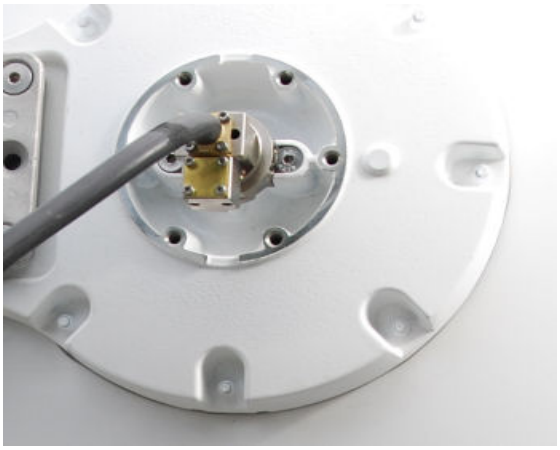
1. Fit the flex waveguide to the remote mount bracket.



2. Fit assembly to pole.



3 Connect the flexible waveguide to the antenna.



4 Remove protective film from coupler ports.



5 Apply silicone grease to the ‘O’ rings of the coupler transitions.

6 Fit the ODUs to the coupler transitions, ensuring that the waveguide interfaces align correctly for vertical or horizontal polarization. Fit both ODUs such that handles are at the top and connectors at the bottom. For asymmetric couplers, check that the ‘MAIN’ and ‘STANDBY’ sides of the coupler can still be identified.



7 Support the flexible waveguide with the waveguide hangers. Do not exceed the flexible waveguide minimum bend radius.



8 Check the finished installation.



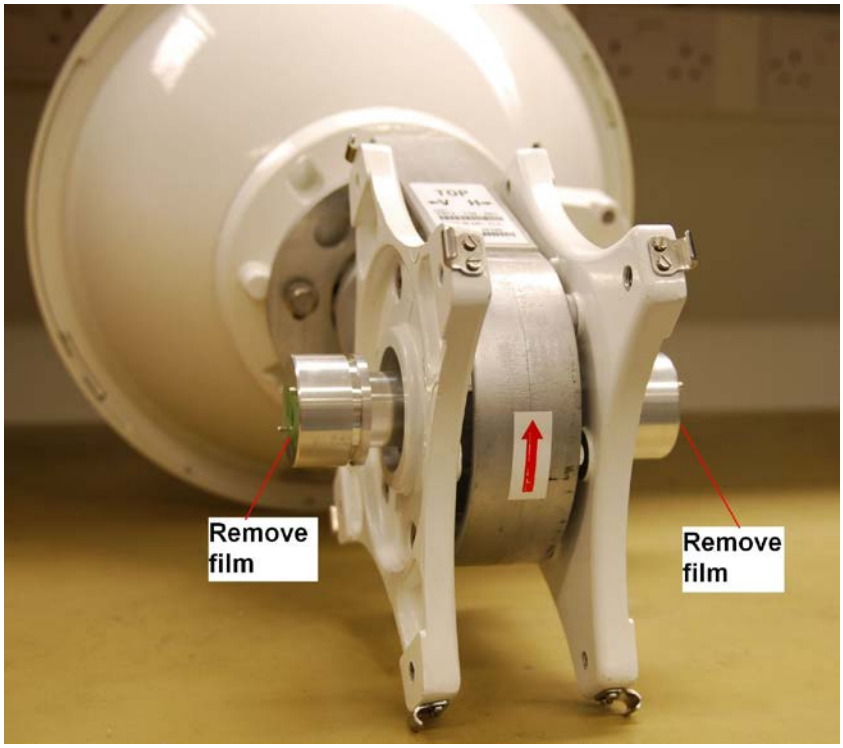
Installing a direct mount dual-polar antenna with two ODUs

Direct mount dual-polar antennas are supplied with an orthogonal mode transducer with two direct-mount interfaces.

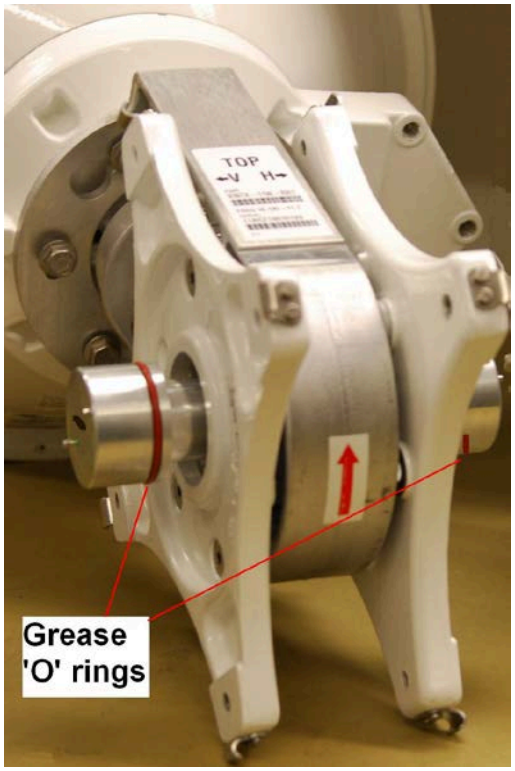
> **NOTE**
> To upgrade any standard antenna to a direct mount dual polar antenna, purchase an orthogonal mount kit (OMK) from Cambium.

To install a direct mount dual-polar antenna with two ODUs, proceed as follows:

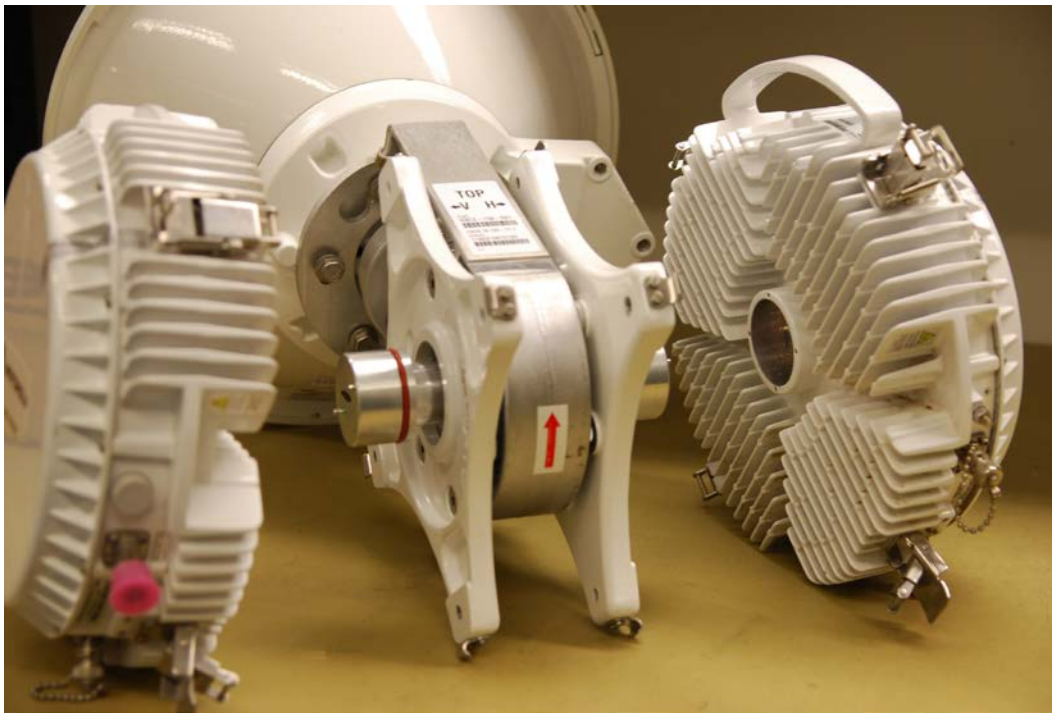
1. Follow the manufacturer's instructions to fit the antenna mounting bracket and fit the antenna to the orthogonal mode transducer.
2. Remove protective film from the ODU transitions.



3 Apply silicone grease to the ‘O’ rings of the ODU transitions.

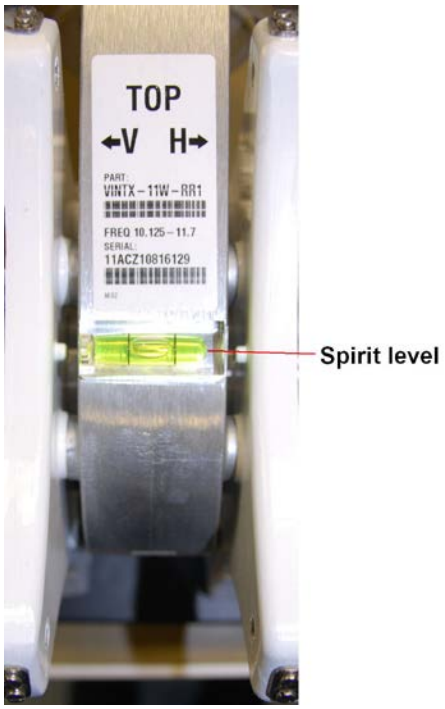


4 Fit the ODUs to the transitions, ensuring that the waveguide interfaces align correctly for vertical or horizontal polarization.



5 Follow the manufacturer’s instructions to attach the assembly to the mast or pole.

6 Place the supplied spirit level on the leveling flat and use it to achieve horizontal alignment of the antenna and ODU assembly.



Installing the IF and ground cables

NOTE
Applies to ODU deployments only.

This section describes how to install the IF cables and how to install grounding and lightning protection.

When installing a 1+1 Hot Standby link, install and ground separate IF cables for the Primary and Secondary ODUs.

When installing a 2+0 link, install and ground separate IF cables for the link A and link B ODUs.

This task consists of the following procedures:

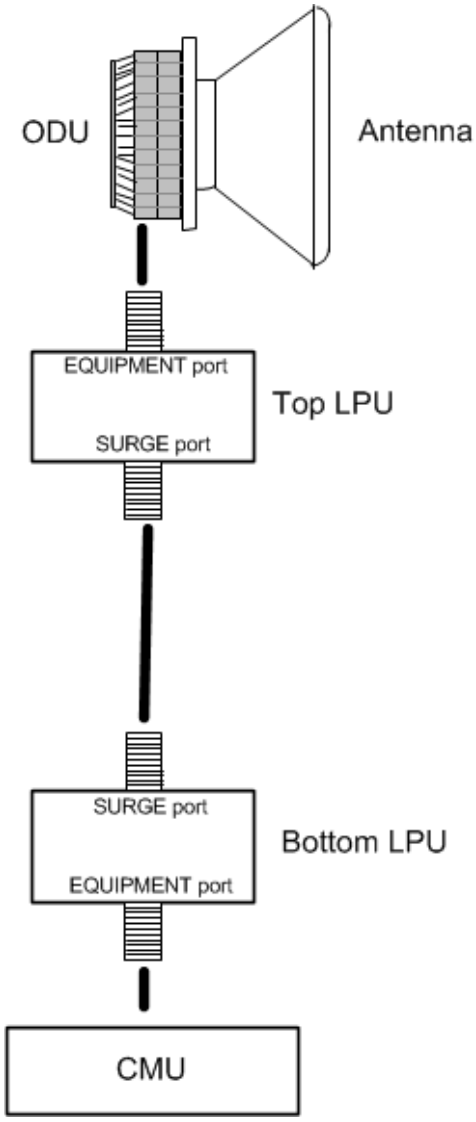
- Preparing IF cables on page 5-38.
- Fitting an N type connector to an IF cable on page 5-38.
- Connecting the ODU to the top LPU on page 5-42.
- Weatherproofing an N type connector on page 5-45.
- Hoisting the main IF cable on page 5-49.
- Installing and grounding the main IF cable on page 5-52.
- Making an IF cable ground point on page 5-54.
- Installing and grounding the IF cable at building entry on page 5-58.

CAUTION
To avoid damage to equipment, observe the following precautions when installing IF and ground cables.

When installing IF and ground cables, observe the following precautions:

- Ensure that the IF and ground cable installation meets the requirements defined in Grounding and lightning protection on page 2-7.
- To provide effective protection against lightning induced surges, install grounding cables without drip loops and pointing down towards the ground.
- To ensure that IF connections are not damaged by water ingress, protect all outdoor IF connectors from the weather with self-amalgamating and vinyl tape.
- Do not connect or disconnect the IF cable when the power supply is applied to the CMU.
- Always ensure the lightning protection units are connected the correct way round (Figure 75).

Figure 75 Correct orientation of LPUs



Preparing IF cables

Prepare the following lengths of IF cable:

- **'ODU-LPU' IF cable**: Use the braided cable assembly supplied in the coaxial cable installation assembly kit (Table 57), as this is pre-fitted with N type connectors. If this is not suitable, cut a short section of IF cable and fit N type connectors to both ends as described in Fitting an N type connector to an IF cable on page 5-38.
- **'Main' IF cable**: Prepare a long section of IF cable to connect the top LPU to the bottom LPU:
  - Cut this to the approximate length required (allowing a bit of surplus), or leave it on the drum so that it can be unwound as the cable is hoisted.
  - Slide one or more hoisting grips onto the top end of the main IF cable, as described in Hoisting the main IF cable on page 5-49.
  - Fit an N type connector to the top end only, as described in Fitting an N type connector to an IF cable on page 5-38.
- **'LPU-CMU' IF cable**: Prepare a short section of IF cable to connect the bottom LPU to the CMU:
  - Cut this to the approximate length required (allowing a bit of surplus).
  - Fit an N type connector to the LPU end only, as described in Fitting an N type connector to an IF cable on page 5-38.

Fitting an N type connector to an IF cable

The crimp tool for the standard N type connector is available from Cambium, see Table 56.

Not all connectors and crimp tools are compatible. If any other type of connector is to be installed, ensure that the correct crimp tool is used.

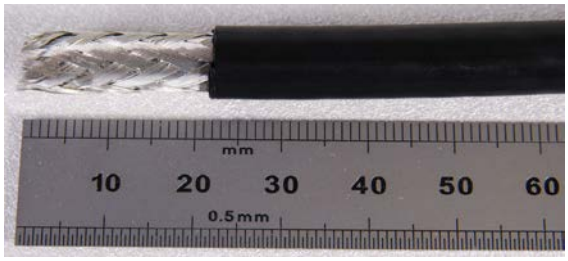
Preparing a cable end

To prepare an IF cable to receive an N type connector, proceed as follows:

1. Check that the correct IF cable crimp tool and connectors are available.



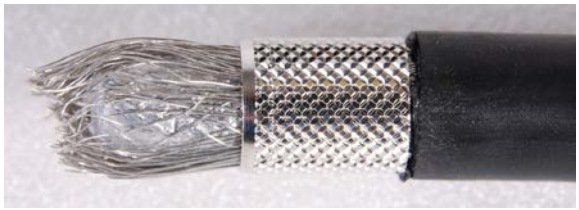
2 Remove 21mm (0.827 inch) of the outer jacket:



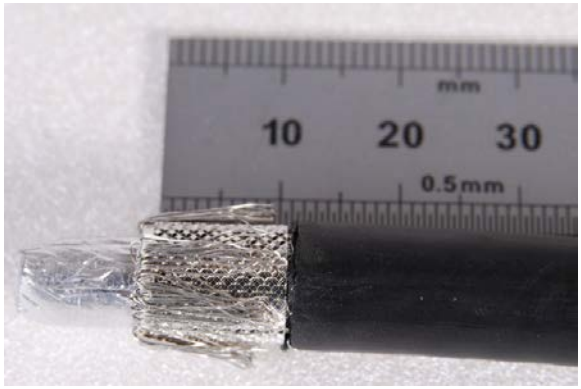
3 Slide ferrule over braid, ensure the chamfer is towards the braid:



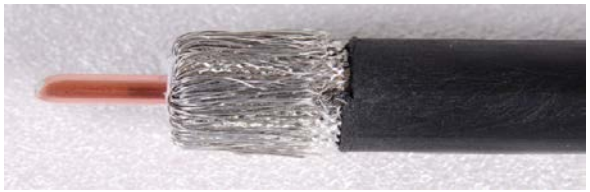
4 Comb braid straight with wire brush:



5 Trim braid back to 9mm (0.354 inch):

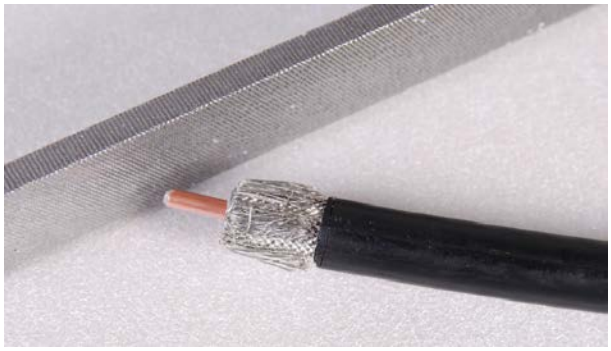


6 Remove foam insulation and trim centre conductor to 6mm (0.236 inch):

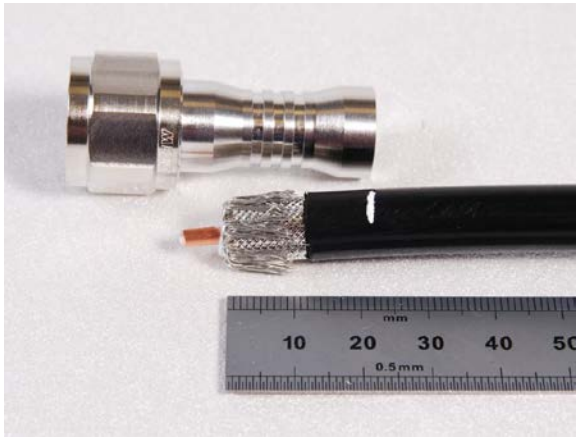


7 Chamfer the centre conductor at a angle of 45°:

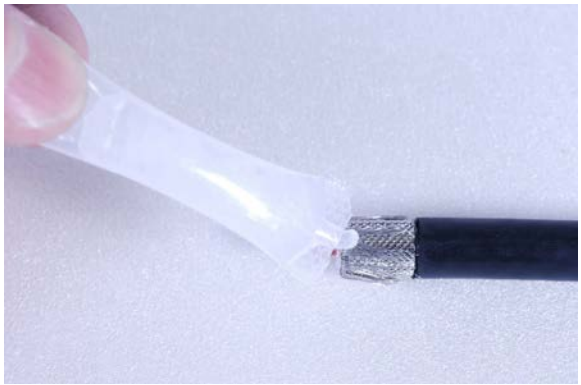
> **⚠ CAUTION**
> Failure to correctly chamfer the centre conductor will cause damage to the connector when assembling the cable into the connector.



8 Mark a line 22 mm from the end of the ferrule:



9 Daub grease onto the braid uniformly:



Crimping a connector

To crimp an N type connector to an IF cable, proceed as follows:

1. Insert the cable into connector. The cable centre conductor must be inserted into the inner contact fingers:

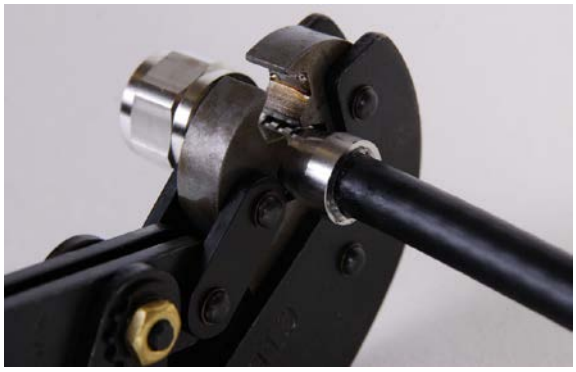


2. Ensure that the cable is not inserted beyond the line marked in Step 8.

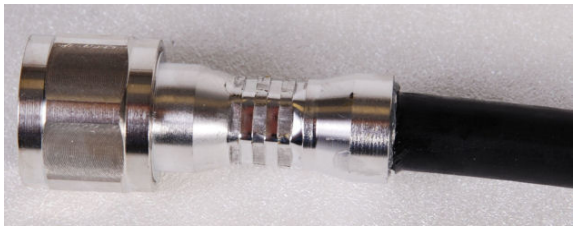
   Crimp the connector body in the area shown:



3. Use the larger of the openings in the crimp tool:



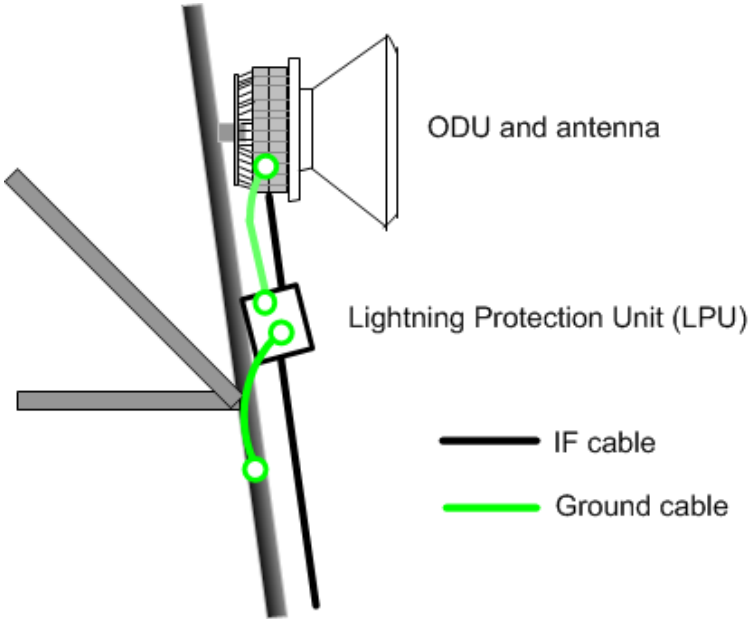
4. Check the finished part:



Connecting the ODU to the top LPU

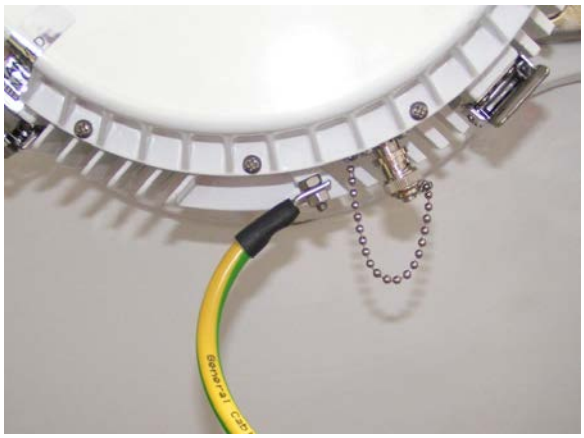
Perform this procedure to connect the ODU to the top lightning protection unit (LPU) via ground and IF cables, and to ground the LPU to the supporting structure (Figure 76).

Figure 76 ODU and top LPU grounding

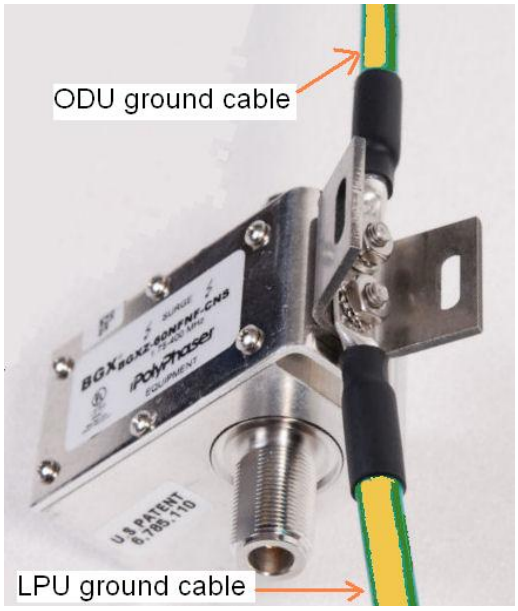


To connect and ground the ODU and top LPU, proceed as follows:

1. Attach one end of the ODU ground cable to the ODU.



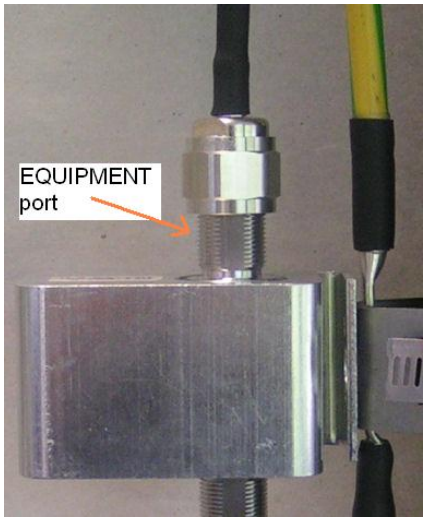
2 Attach the other end of the ODU ground cable to the top LPU, under the LPU mounting nut. Attach one end of the LPU ground cable to the LPU, under the LPU mounting nut.



3 Attach one end of the ODU-LPU IF cable to the ODU.



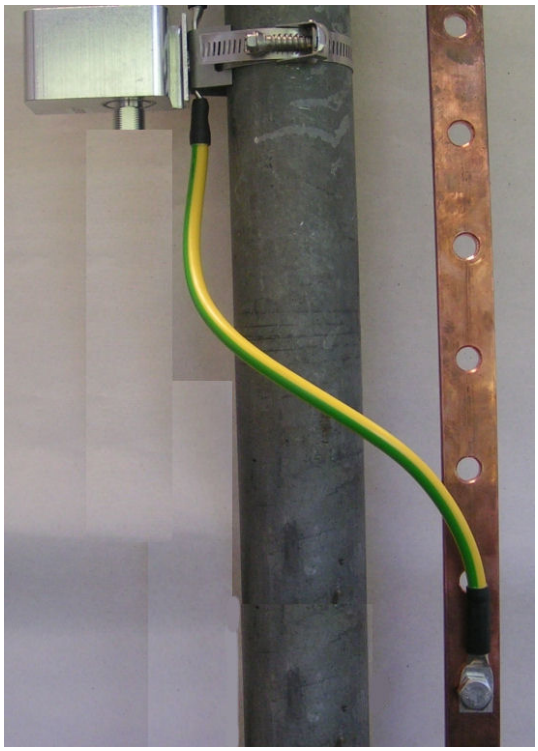
4 Attach the other end of the ODU-LPU IF cable to the EQUIPMENT port of the top LPU.



5 Mount the top LPU on the supporting structure.

6 Route and fasten the ODU ground cable and ODU-LPU IF cable. The ground cable should be routed downwards without any loops.

7 Attach the other end of the LPU ground cable to the grounding bar of the supporting structure.



8 Protect the N type connectors at the ODU and LPU from the weather by applying self-amalgamating and PVC tape, as described in Weatherproofing an N type connector on page 5-45.

Weatherproofing an N type connector

Use this procedure to weatherproof the N type connectors fitted to the ODU and LPU.

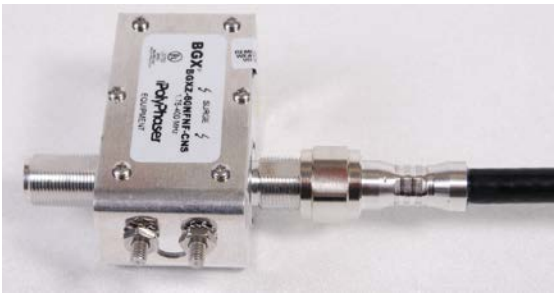
Before weatherproofing the connectors, ensure that the installation has been tested as described in Testing the ODU and IF cable on page 5-60. These tests require connection and disconnection of the IF cables at various places.

NOTE

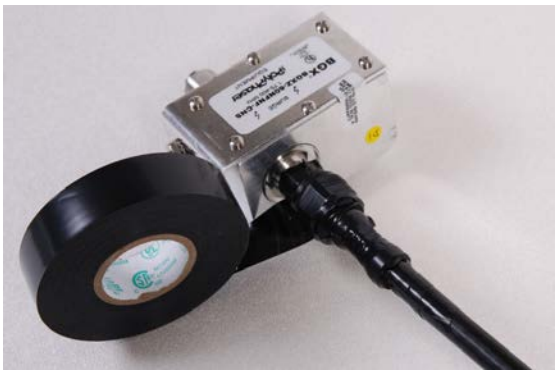
Tighten N type connectors using a torque wrench, set to 1.7 Nm (15 lb in). If a torque wrench is not available, finger tighten the N type connectors.

To weatherproof an N type connector, proceed as follows:

1 Ensure the connection is tight, using a torque wrench (if available):



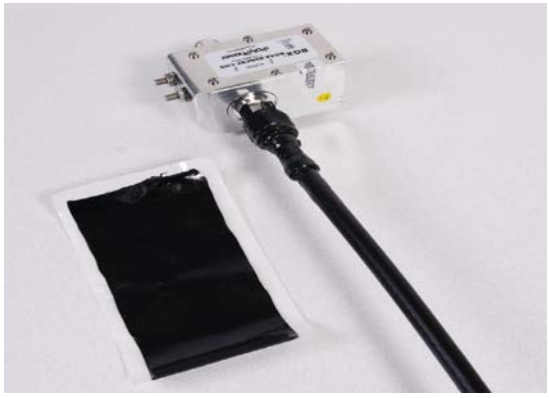
2 Wrap the connection with a layer of 19 mm (0.75 inch) PVC tape, starting 25 mm (1 inch) below the connector body. Overlap the tape to half-width and extend the wrapping to the body of the LPU. Avoid making creases or wrinkles:



3 Smooth tape edges:



4 Cut a 125mm (5 inches) length of rubber tape (self amalgamating):



5 Expand the width of the tape by stretching it so that it will wrap completely around the connector and cable:



6 Press the tape edges together so that there are no gaps. The tape should extend 25mm (1inch) beyond the PVC tape:



7 Wrap a layer of 50 mm (2 inch) PVC tape from bottom to top, starting from 25 mm (1 inch) below the edge of the self-amalgamating tape, overlapping at half width.



8 Repeat with a further four layers of 19 mm (0.75 inch) PVC tape, always overlapping at half width. Wrap the layers in alternate directions:

Second layer: top to bottom.

Third layer: bottom to top.

Fourth layer: top to bottom.

Fifth layer: bottom to top.

The bottom edge of each layer should be 25 mm (1 inch) below the previous layer.



9 Completed weatherproof connection:



Hoisting the main IF cable

Use hoisting grips to hoist the main IF cable safely up a tower or building and provide permanent support so that mechanical connection to an antenna can be made. The correct hoisting grip for CNT-400 IF cable is Cambium part number 07009304001, used with the correct crimp tool SG-IT (Andrew part number 243333).

WARNING

Failure to obey the following precautions may result in injury or death.

Observe the following precautions:

- Use the hoisting grip to hoist one cable only. Attempting to hoist more than one cable may cause the hoisting grip to break or the cables to fall.
- Do not use the hoisting grip for lowering cable unless the clamp is securely in place.
- Do not reuse hoisting grips. Used grips may have lost elasticity, stretched, or become weakened. Reusing a grip can cause the cable to slip, break, or fall.
- Use hoisting grips at intervals of no more than 60 m (200 ft).
- Use the proper hoisting grip for the cable being installed. If the wrong hoisting grip is used, slippage or insufficient gripping strength will result.

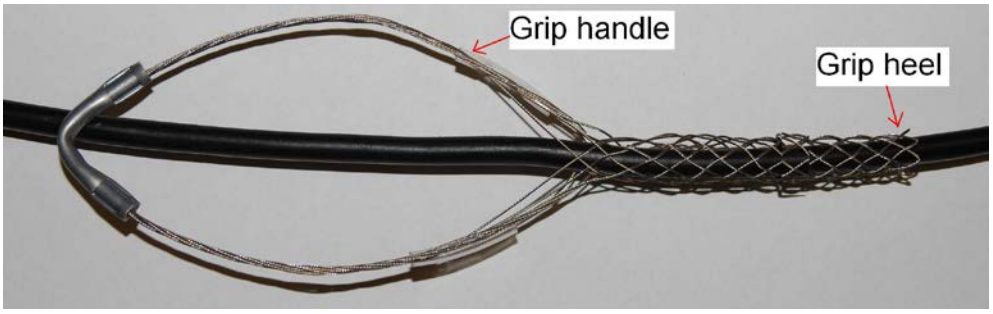
Attaching the hoisting grip

NOTE

Attach one or more hoisting grips to the main IF cable before fitting the N type connector to the top end (as described in Preparing IF cables on page 5-38). Attach one additional hoisting grip for each 60 m (200 ft) of cable.

To attach a hoisting grip to the main IF cable, proceed as follows:

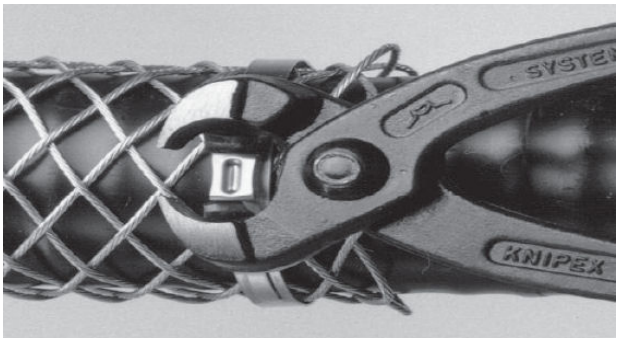
1 Compress the grip ends towards each other and slide the grip heel (woven end) onto the cable (see photo). Place the hoisting grip(s) at the proper location on the cable before attaching the connector. Allow a sufficient length of cable leader to reach the antenna connector when cable hoisting and attachment of the grip handle is completed. Hold the heel with one hand and firmly slide the other hand along the grip to tighten it.



2 Slide the clamp onto the grip and position it 25 mm (1”) from the heel.



3 Crimp the clamp with Andrew crimping tool 243333 at each hoisting grip clamp location.



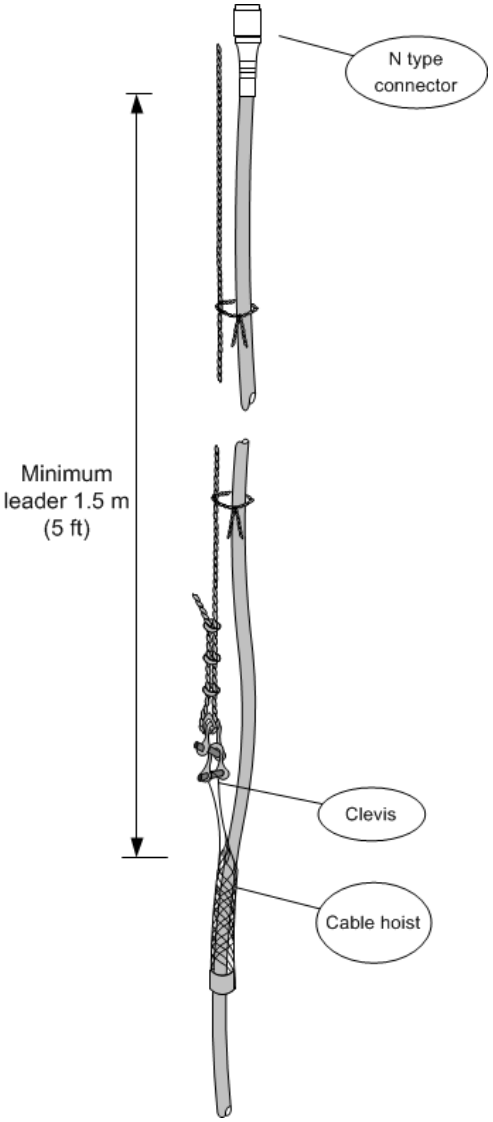
Using the hoist line

WARNING

Maintain tension on the hoisting grip during hoisting. Loss of tension can cause dangerous movement of the cable and result in injury or death to personnel on or near the tower. Also, do not release tension on the grip until after the cable has been fastened to the tower members.

Attach the hoist line to the grip (Figure 77). Tie the cable leader to the hoist line so that the leader does not dangle. Apply tension slowly to the hoist line, allowing the hoisting grip to tighten uniformly on the cable. Hoist the main IF cable up to the ODU.

Figure 77 Using the hoist line

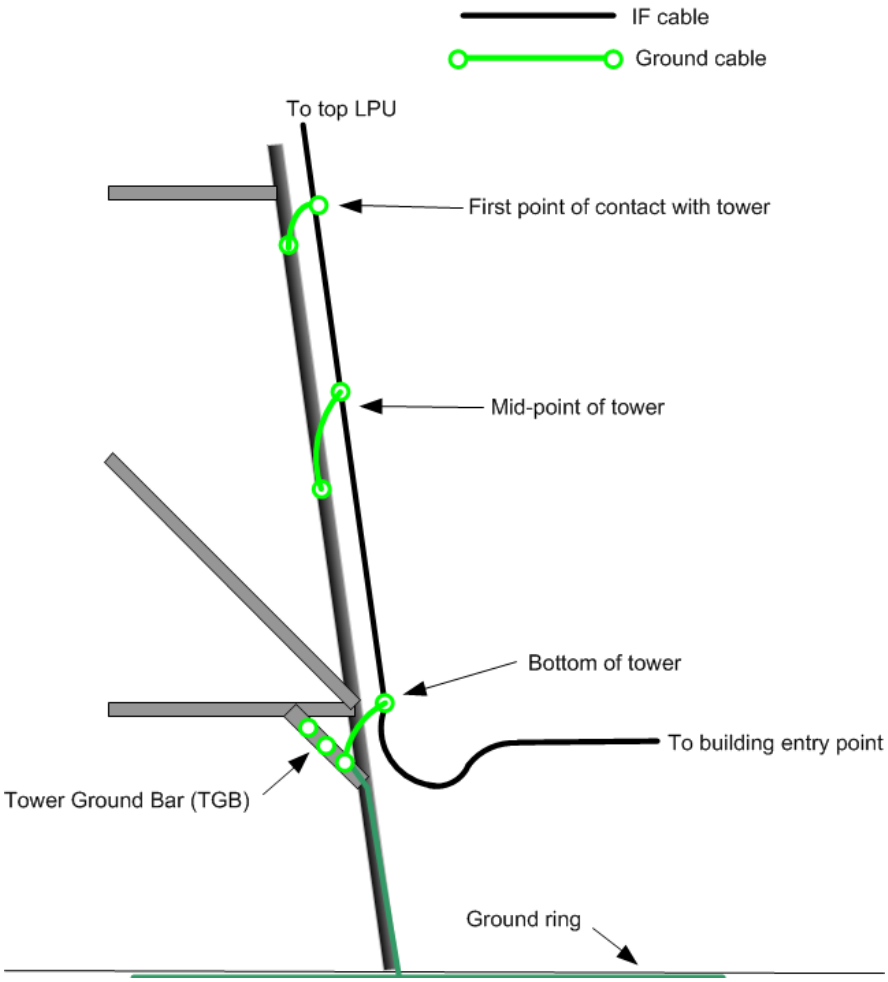


When the cable is in position, fasten the grip handle to a tower member and remove the hoist line.

Installing and grounding the main IF cable

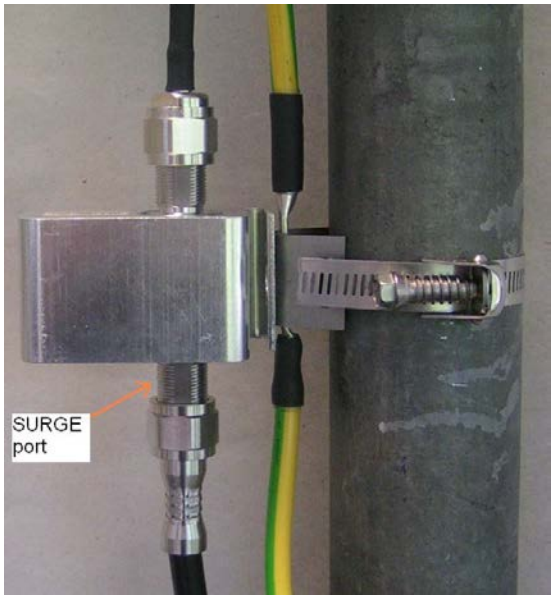
Perform this procedure to install and ground the IF cable from the top LPU to the building entry point (Figure 78). The IF cable must be grounded at the points specified in Protection requirements for a mast or tower installation on page 2-11.

Figure 78 IF cable grounding on a mast or tower



To install and ground the main IF cable, proceed as follows:

1. Attach the N type connector at the top end of the main IF cable to the SURGE port of the top LPU.



2. Protect the N type connectors on the LPU from the weather by applying self-amalgamating and PVC tape, as described in Weatherproofing an N type connector on page 5-45.

3. Lay the main IF cable as far as the building entry point, ensuring there is enough length to extend through the wall of the building to the bottom LPU.

4. Attach the main IF cable to the supporting structure using the cable ties provided.

5. Ground the IF cable at the points specified in Protection requirements for a mast or tower installation on page 2-11.

   Follow the procedure Making an IF cable ground point on page 5-54.

Making an IF cable ground point

Perform this task to connect the screen of the IF cable to the metal of the supporting structure using a cable grounding kit.

The cable grounding kit for 1/4” and 3/8” cable (Figure 26) contains the following components:

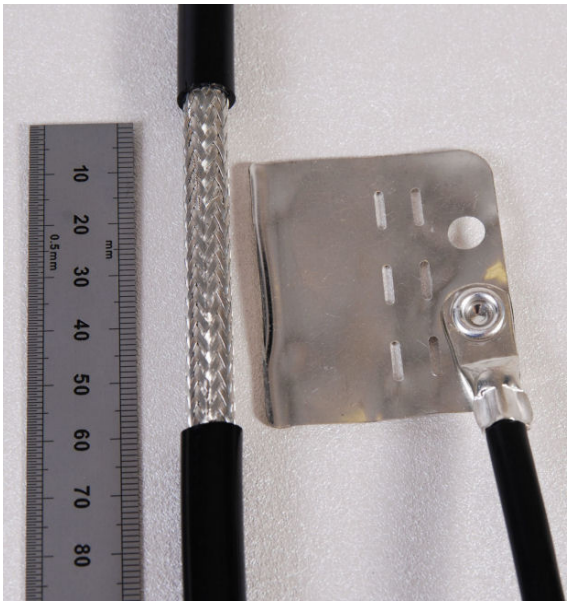
- 1 x grounding cable with grounding 2 hole lug fitted (M10)
- 1 x self Amalgamating tape
- 1 x PVC tape
- 3 x tie wraps
- 2 x bolt, washer and nut

⚠ CAUTION

Install ground cables installed without drip loops and pointing down towards the ground, otherwise they may not be effective.

To ground the IF cable to a metal structure using the Cambium grounding kit (part number 01010419001), proceed as follows:

1. Remove 60 mm (2.5 inches) of the IF cable outer jacket:



2 Cut 38 mm (1.5 inches) of rubber tape (self amalgamating) and fit to the ground cable lug. Wrap the tape completely around the lug and cable:



3 Fold the ground wire strap around the drop cable screen and fit cable ties.



4 Tighten the cable ties with pliers.



Cut the surplus from the cable ties.

5 Cut a 38 mm (1.5 inches) section of self-amalgamating tape and fit to the ground cable lug. Wrap the self-amalgamating tape completely around the lug and cable.



6 Use the remainder of the self-amalgamating tape to wrap the complete assembly. Press the tape edges together so that there are no gaps:



7 Wrap a layer of PVC tape from bottom to top, starting from 25 mm (1 inch) below and finishing 25 mm (1 inch) above the edge of the self-amalgamating tape, over lapping at half width.



8 Repeat with a further four layers of PVC tape, always overlapping at half width. Wrap the layers in alternate directions:

Second layer: top to bottom.

Third layer: bottom to top.

Fourth layer: top to bottom.

Fifth layer: bottom to top.

The edges of each layer should be 25mm (1 inch) above (A) and 25 mm (1 inch) below (B) the previous layer.



9 Prepare the metal grounding point of the supporting structure to provide a good electrical contact with the grounding cable clamp. Remove paint, grease or dirt, if present. Apply anti-oxidant compound liberally between the two metals.

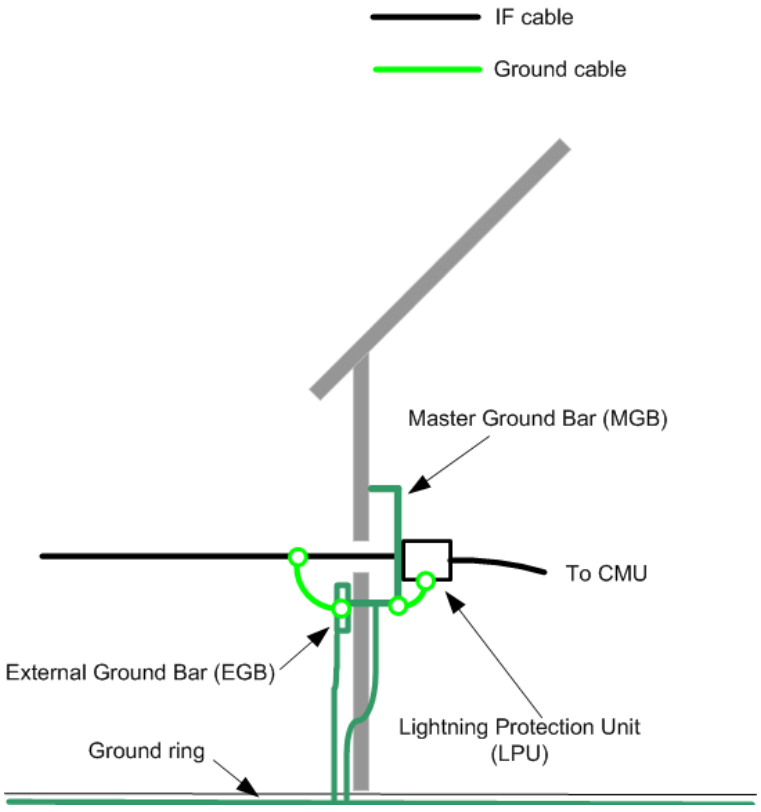
10 Clamp the bottom lug of the grounding cable to the supporting structure using site approved methods.

> **NOTE**
> Use a two-hole lug secured with fasteners in both holes. This provides better protection than a single-hole lug.

Installing and grounding the IF cable at building entry

Perform this procedure to install and ground the IF at the building (or cabinet) entry point (Figure 79).

Figure 79 Grounding at building entry



To run the IF cable into the building, proceed as follows:

1. Make an entry point into the building and run the main IF cable into the building.
2. Ground the IF cable to the external ground bar outside the building entry point, as described in Making an IF cable ground point on page 5-54.
3. Install the bottom LPU inside the building entry point.
4. Ground the bottom LPU to the master ground bar.
5. Cut any surplus length from the bottom end of the main IF cable and fit an N type connector, as described in Fitting an N type connector to an IF cable on page 5-38.
6. Connect the main IF cable (from the ODU) to the SURGE port of the bottom LPU.
7. Connect the LPU-CMU IF cable to the EQUIPMENT port of the bottom LPU and run it to the location of the CMU.

Testing the ODU and IF cable

> **NOTE**
> Applies to ODU deployments only.

This section describes how to perform pre-power tests on the ODU, LPUs and the IF cable.

Recommended pre-power tests

After installation of the ODU, LPUs and the IF cable, but before connecting and applying power to the CMU, perform the following tests:

- Cable loss with ODU disconnected:

  Confirm that the total cable loss, including loss from the LPUs, is within acceptable limits.

- Cable loss with the ODU connected:

  Confirm that the cable contains no short circuit or open circuit.

- Distance to fault (DTF) return loss with the ODU connected:

  Confirm the position of the LPUs in the cable run and confirm that there are no other points of discontinuity in the cable. To detect any degradation over time, compare a current plot to a previously recorded plot, if available.

Test equipment

Use an RF cable analyzer such as an Anritsu ‘Site Master’ to confirm that the installed cable between the ODU and the CMU has the correct loss and does not have any short or open circuits. If the cable is faulty, use this equipment to identify the location of a fault in the cable.

Figure 80 is an example of a cable analyzer that is suitable for performing the tests described in this section.

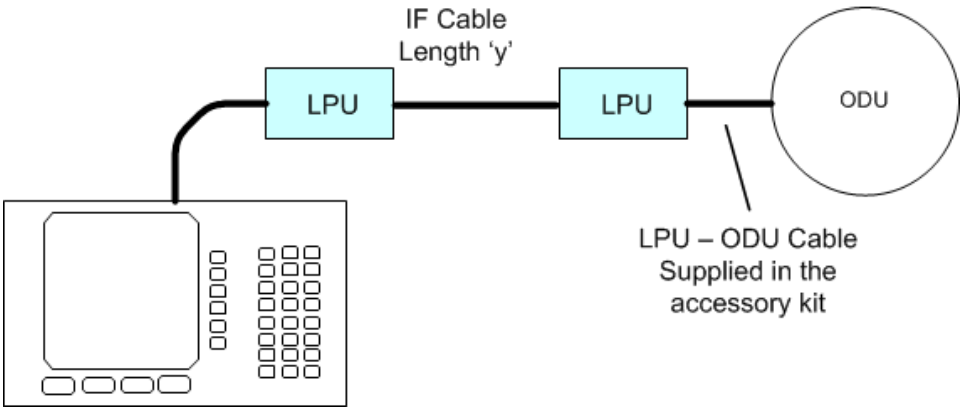
Figure 80 Example of a cable analyzer



Test preparation

Set up the equipment to perform the pre-power tests. Figure 81 is an example to show how this is done. In this example, there is a short length of cable from the analyzer (in place of the CMU) to the first LPU, a length of cable ‘y’ from the first LPU to the second LPU (at the top of the tower) and a short length of cable from the second LPU to the ODU (0.7m long supplied in the accessory kit).

Figure 81 Example of the cable test



NOTE

Perform these tests in conjunction with the test equipment manufacturer’s instructions.

To prepare for pre-power testing, proceed as follows:

1. Connect the analyzer to the first LPU (Figure 81).
2. Connect the first LPU to the second (Figure 81).
3. Check that the second LPU is disconnected from the cable that leads to the ODU (Figure 81) (the second LPU and ODU are reconnected during testing).
4. Power on the analyzer.

When these preparations are complete, perform the following tests:

- Testing cable loss on page 5-62.
- Measuring distance to fault on page 5-67.

Testing cable loss

The purpose of this test is to ensure that the total cable loss is within acceptable limits.

Before performing this test, ensure that the test equipment is set up as described in Test preparation on page 5-61.

To measure cable loss, proceed as follows:

1. Select the ‘cable loss-one port’ mode of the cable analyzer (Figure 80).
2. Set the frequency of measurement to:

   F1 = 350MHz

   F2 = 400MHz.
3. Calibrate the instrument for the selected frequencies, using the correct calibration kit.
4. Before connecting the ODU, obtain a plot of cable loss and check that it is within the expected limits for the given cable length (Table 215). Compare it to examples of good installations (Figure 82 and Figure 84).
5. Connect the ODU.
6. Observe the effect of the ODU connection on the plot of cable loss.

   Compare it to examples of good installations (Figure 83 and Figure 85).

   If there is little or no change to the plot when the ODU is connected, it indicates a short or open circuit on the cable.
7. Keep a copy of the cable loss plots so that they can be compared with subsequent plots to determine if there is any degradation with time.

Cable loss example using a 17 meter cable

This example is for a cable run consisting of the following:

- 0.7m cable from the test equipment to the first LPU.
- The first LPU.
- 17m of cable between the two LPUs (length ‘y’ in Figure 81).
- The second (mast mounted) LPU.
- 0.7m of cable from the LPU to ODU.

When performing steps 4 to 6 above, compare the ‘before’ and ‘after’ plots of cable loss:

- Figure 82 is a plot of cable loss taken before the ODU was connected. The plot shows an average cable loss of 1.96 dB. This can be compared with the expected result in Table 215. For a cable length of approximately 19m (17m + 0.7m + 0.7m) with two LPUs, the table result is 1.9 dB, which is within the expected tolerance of +/- 10%.
- Figure 83 is a plot of cable loss taken after the ODU was connected.

Figure 82 Cable loss plot for a 17 meter cable with no ODU

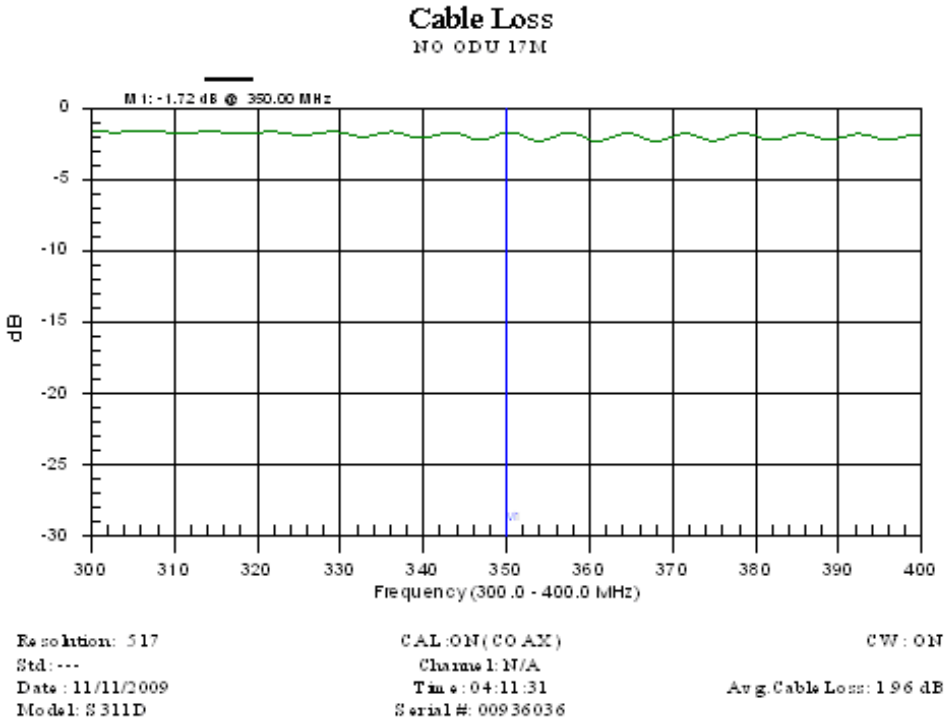
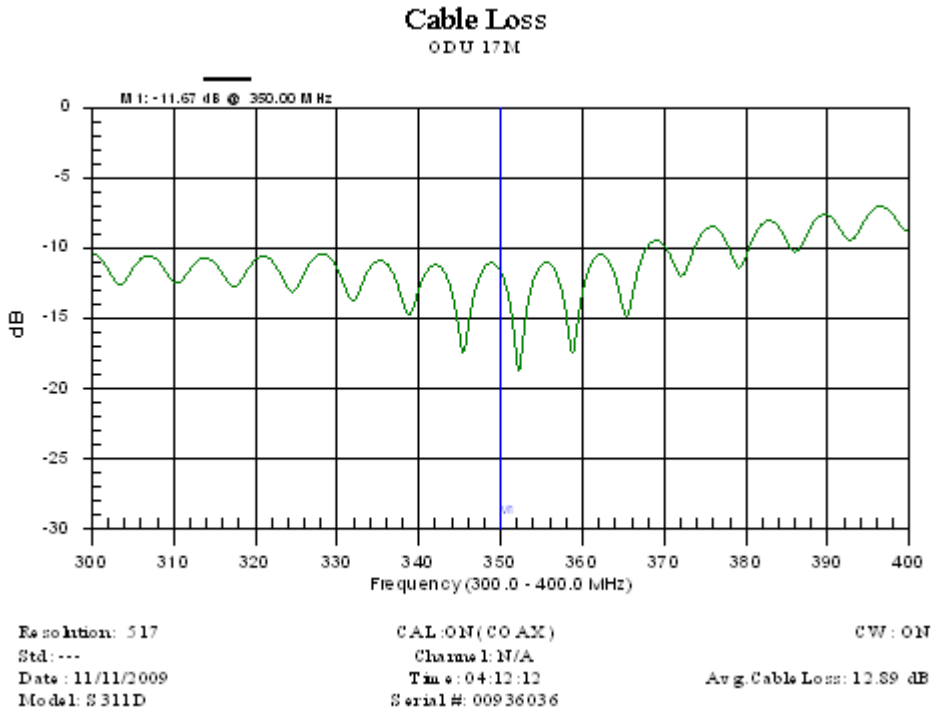


Figure 83 Cable loss plot for a 17 meter cable with ODU connected



Cable loss example using a 100 meter cable

This is similar to the above example, except that there is now 100m of cable between the two LPUs (length ‘y’ in Figure 81). It shows similar results:

- Figure 84 is a plot of cable loss taken before the ODU was connected.
- Figure 85 is a plot of cable loss taken after the ODU was connected.

Figure 84 Cable loss plot for a 100 meter cable with no ODU

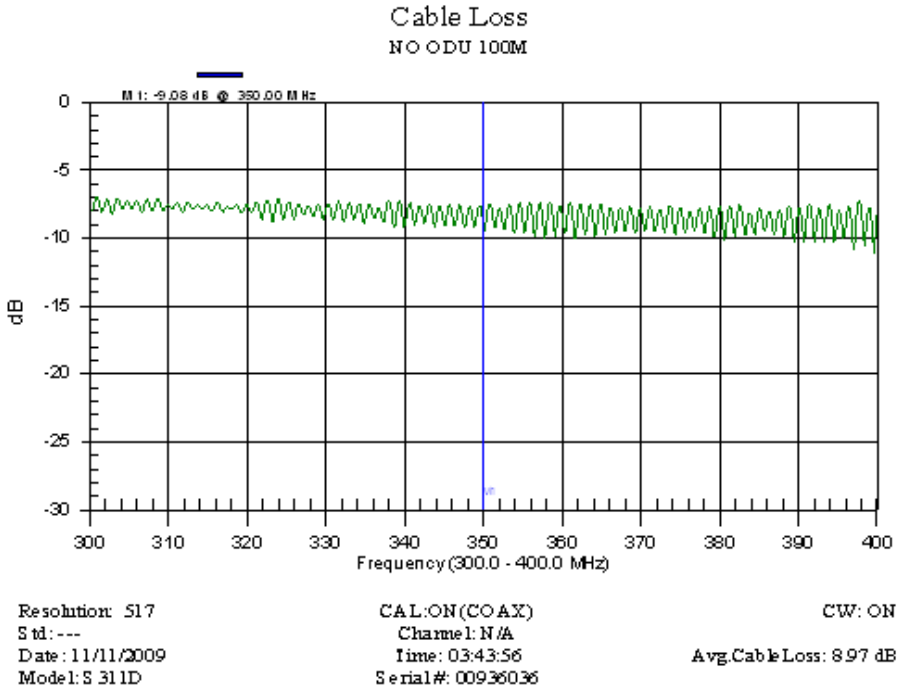
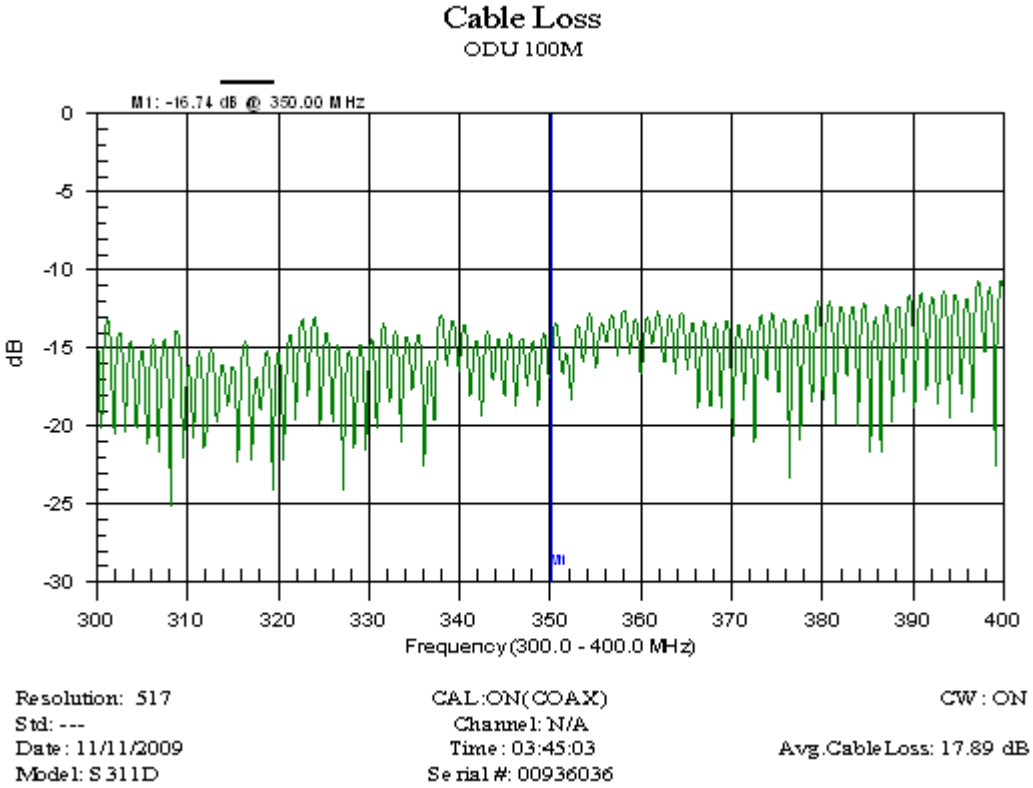


Figure 85 Cable loss plot for a 100 meter cable with ODU connected



Expected cable loss

Table 215 quotes the expected cable loss for given cable lengths when the ODU is not connected. All loss figures have a tolerance of plus or minus 10%, for example, 1.76 dB means that the loss is expected to be between 1.58 and 1.94 dB.

Table 215 Expected cable loss when ODU is not connected

Cable Length (meters)	Cable Loss (+/- 10%) at 350 MHz (dB)	Cable Loss (+/- 10%) with two Lightning Protection Units fitted, at 350 MHz (dB)
1	0.08	0.3
2	0.15	0.37
3	0.23	0.45
4	0.31	0.53
5	0.39	0.61
6	0.46	0.68
7	0.54	0.76
8	0.62	0.84
9	0.69	0.91
10	0.77	0.99
20	1.54	1.76
30	2.31	2.53
40	3.08	3.3
50	3.85	4.1
100	7.7	7.92

Measuring distance to fault

The distance to fault (DTF) test is used as a means of characterizing the cable installation, but can also be used to determine the location of a fault in an installation.

Before performing this test, ensure that the test equipment is set up as described in Test preparation on page 5-61.

To measure distance to fault, proceed as follows:

1. Select the 'DTF-return loss' mode of the cable analyzer (Figure 80).
2. Select 'DTF Aid'.
3. Use the up/down key to select and set the following:

   Cable type - select LMR400 (similar to CNT-400) or LMR600 (similar to CNT-600) as appropriate.

   F2 - select the highest frequency possible for the greatest resolution, 1600 MHz.

   D1 and **D2** - set as appropriate for the specific installation.
4. Recalibrate the instrument.
5. Before connecting the ODU, obtain a plot of DTF loss. Compare it to an example of a good installation (Figure 86).
6. Connect the ODU.
7. Observe the effect of the ODU connection on the DTF plot. Compare it to an example of a good installation (Figure 87).
8. Keep a copy of the DTF plots so that they can be compared with subsequent plots to determine if there is any degradation with time.

NOTE

The absolute readings of DTF should be read with care, as many different variables affect both distance and amplitude accuracy.

DTF return loss example

This example shows typical DTF return loss in a good installation. The distances from the test equipment to first LPU (marker M2), and then the second LPU (marker M3) are clearly shown. The cable between them shows **no** discontinuity. There are two plots:

- Figure 86 is a plot of DTF return loss before the ODU is connected. The final peak (marker M1) is the position of the cable open circuit.
- Figure 87 is a plot of DTF return loss after the ODU is connected. The final peak remains in the same position but is now reduced in amplitude because less signal is reflected, as a consequence of the better match of the ODU.

Figure 86 DTF plot for a 17 meter cable with no ODU

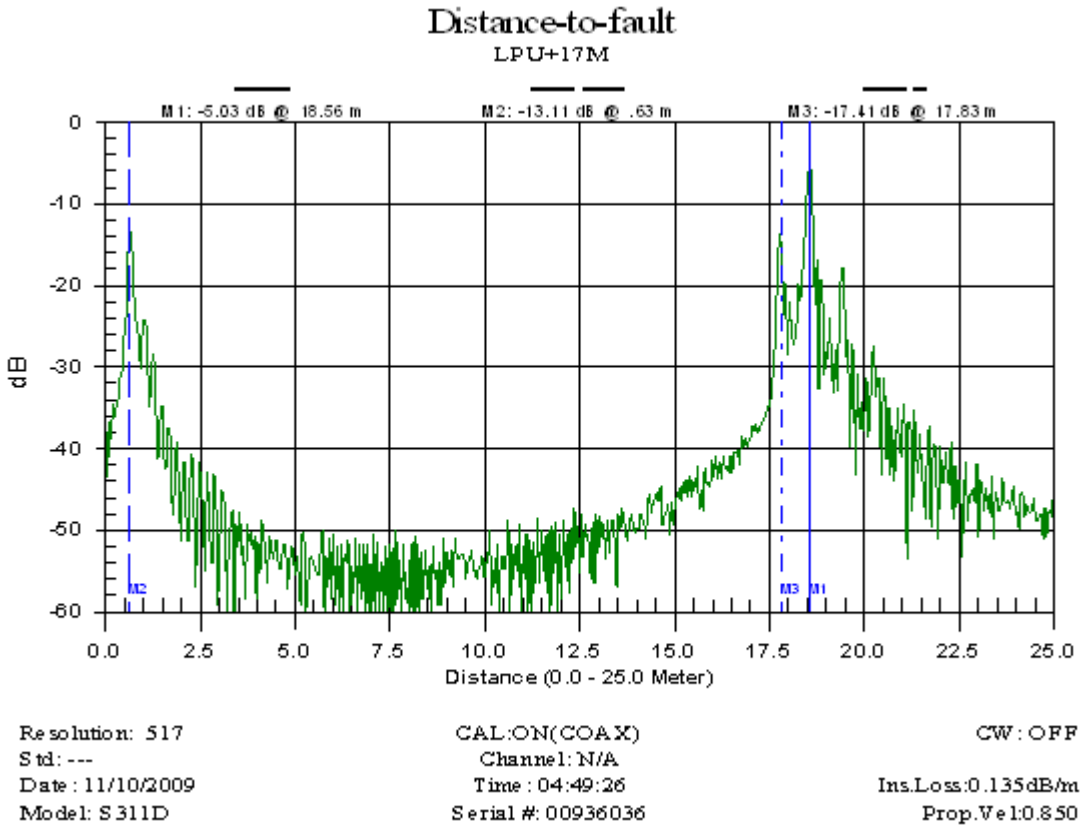
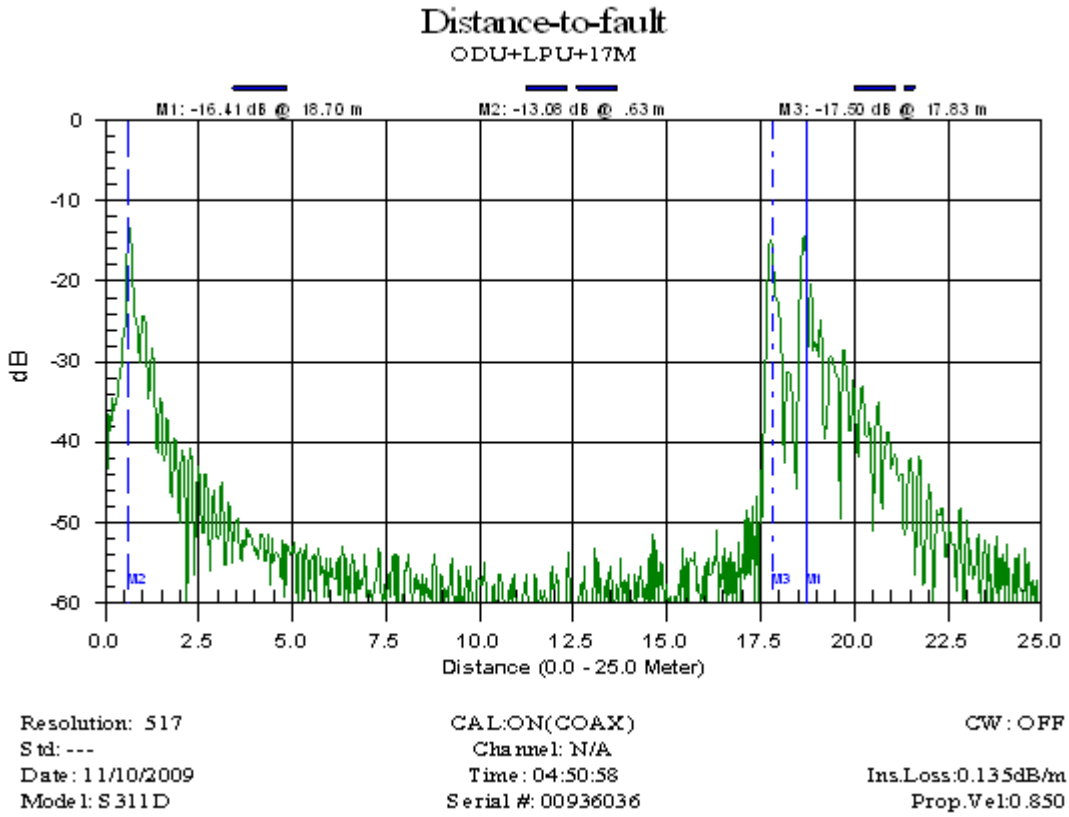


Figure 87 DTF plot for a 17 meter cable with ODU connected



Installing antennas and IRFUs

> **NOTE**
> Applies to IRFU deployments only.

This section describes how to install an IRFU with antenna and waveguide.

> **NOTE**
> Install the antenna and flexible waveguide by following their manufacturers' instructions. The waveguide must be long enough to connect to the IRFU branching unit in its rack.

Preparation

Before installing the IRFU, ensure the following are provided:

- IF cable for CMU and IRFU (Cambium part number 30009403001).
- A -48 V dc power source.
- Access to the building ground terminal.
- All required tools (Table 216).

Table 216 Tools required for IRFU installation

Item	Required specifications	Where used
Screwdriver	Phillips #2, medium tip	Throughout
Allen key	For #8-32 socket-head screws	For connecting the flexible waveguide to the IRFU
Multimeter	With ohm meter	For connecting the CMU to the IRFU
Miscellaneous tools for installing connectors on the CMU to IRFU coaxial cable	Refer to the manufacturer documentation provided with the connector	
Torque wrench for SMA connectors	5/16, set to 0.1 kg•m (9.0 lb-inch)	

Installing the IRFU in the rack

NOTE

Allocate a free space of at least 0.4 RMS (18 mm or 0.7 in) between the bottom of the IRFU bracket and the top of the CMU and, 1.3 RMS (58 mm or 2.3 in) between two IRFU shelves.

NOTE

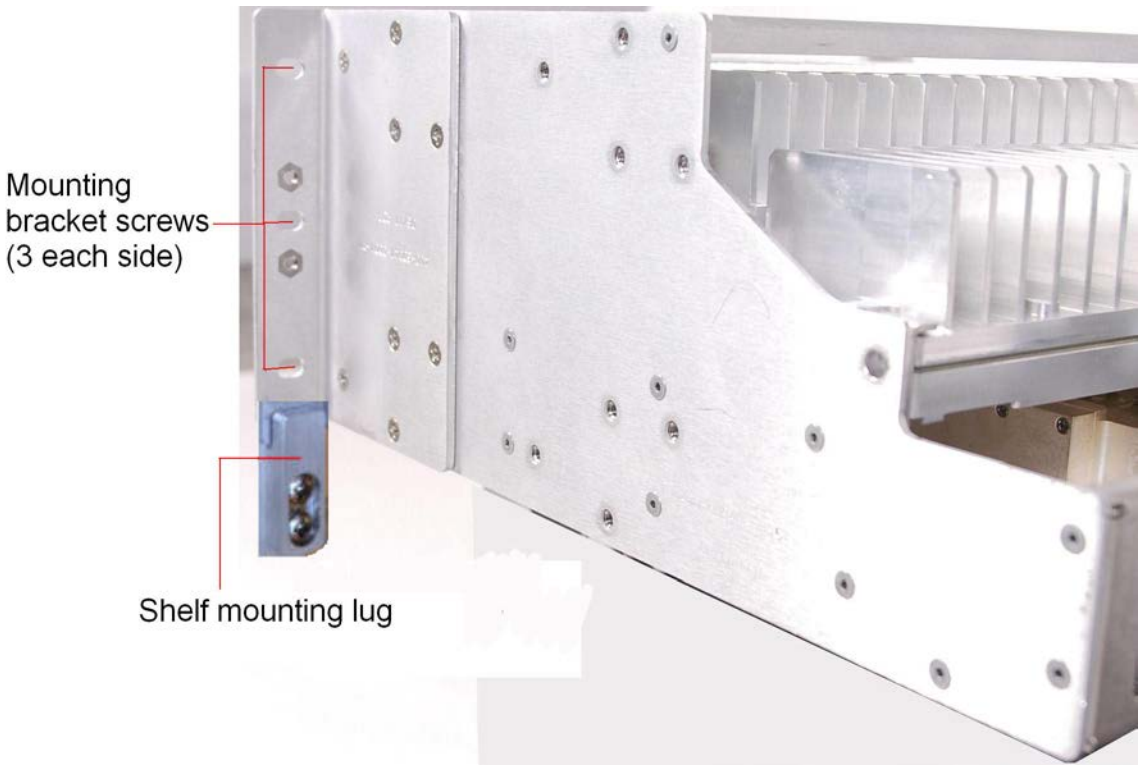
Mounting brackets can be assembled for either ETSI or NEBS (ANSI) rack-mounting.

WARNING

To minimize risk of injury, use two persons to place a fully assembled IRFU (weighing approximately 12 kg) in the rack.

Install the shelf mounting lugs (2) using the machine screws provided. Leave these lugs in place for holding the IRFU during installation. Starting with the two top screws, secure the six mounting bracket screws to the rack (Figure 88).

Figure 88 IRFU rack mounting



Connecting the flexible waveguide to the IRFU

To connect the flexible waveguide from the antenna to the IRFU branching unit (BU), proceed as follows:

1. Remove the protection cap from the BU mating flange (Figure 89).
2. Connect the flanged end of the flexible waveguide to its mating flange on the BU, using the eight socket-head screws provided. Refer to Table 217 for the waveguide and flange specifications.
3. Install the correct flange gasket according to the type of waveguide mating flange (not supplied).
4. Check that the waveguide has been installed according to manufacturer's instructions, with sealed ends and a pressure window.
5. Pressurize the waveguide with dry air (using an appropriate dehydrator) according to manufacturer's instructions.

Figure 89 Partial rear view of IRFU with waveguide port



Table 217 IRFU waveguide and flange specifications

Band (GHz)	Waveguide	Flange type	Flange holes
L6 and U6	WR-137	CPR-137G	Tapped for #8-32 screws
7 and 8	WR-112	CPR-112G	
11	WR-90	CPR-90G	

Connecting the CMU cables to the IRFU

Connect the CMU to the IRFU using the supplied IF cable (Cambium part number 30009403001) (Figure 90). For 1+1 and 2+0 links, repeat for the second transceiver unit and CMU.

Figure 90 Connecting the coaxial cable to the IRFU



Grounding the IRFU

Ground the IRFU by connecting a 4.11 mm (6 AWG) copper cable from any one of the grounding terminals of the IRFU shelf (Figure 91 and Figure 92) to the building grounding system.

Figure 91 IRFU grounding terminal (front option)

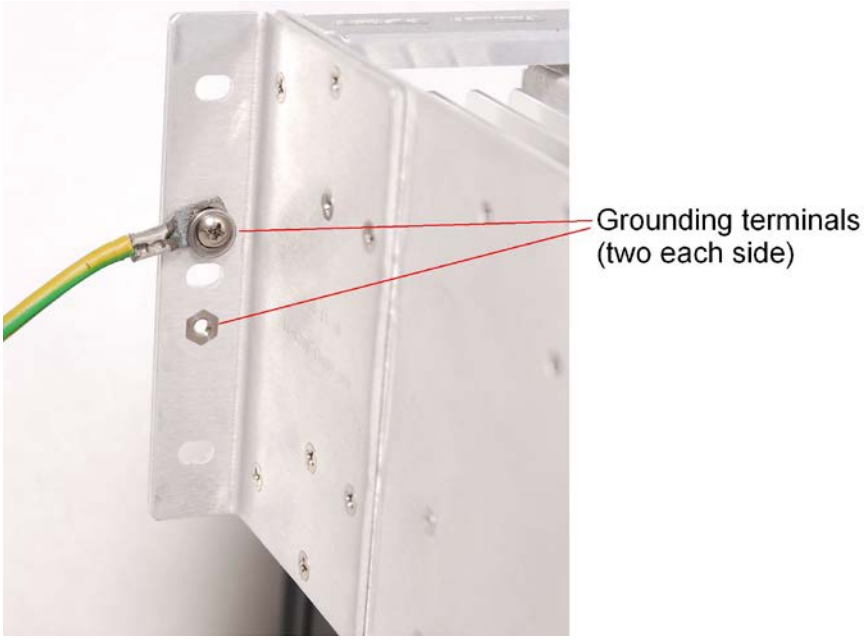
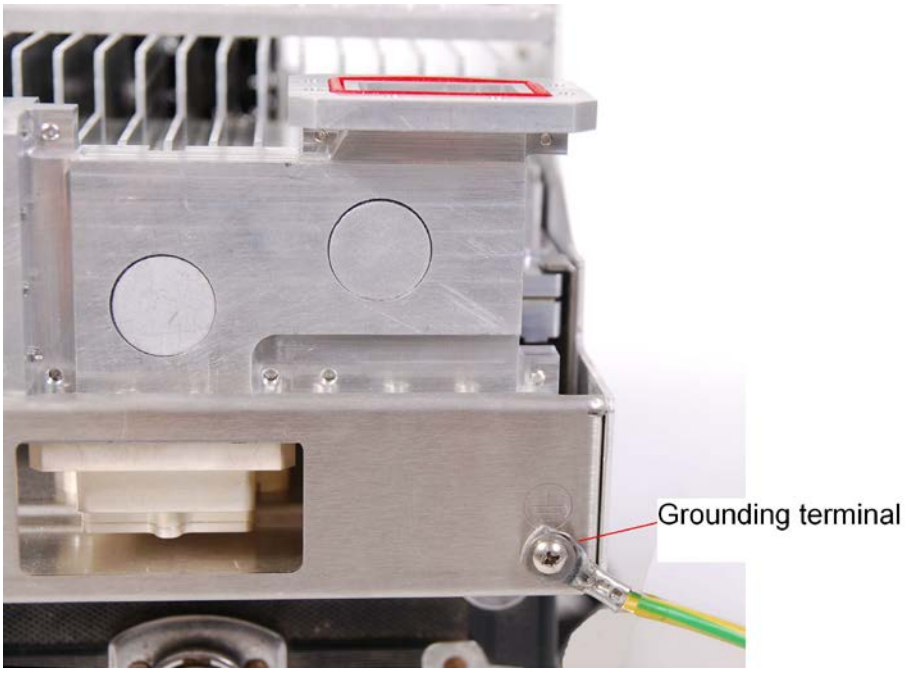


Figure 92 IRFU grounding terminal (rear option)



⚠ CAUTION

Safety requirements for grounding:

It is very important that the path of lowest resistance goes directly to the main ground point.

The ground conductor resistance needs to be less than 0.5 Ohm.

Do not connect other equipment to the same grounding cable as the IRFU. Each piece of equipment at the site should have a separate grounding cable to a common very low resistance main ground point.

Connect the equipment directly to the DC supply system grounding electrode conductor or to a bonding jumper from a grounding terminal bar, or bus to which the DC supply grounding electrode is connected.

⚠ CAUTION

Provide fusing according to Local and National Electrical Codes. Fuse rating must be: 4 A for -48 V operation.

Connecting power to the IRFU

Connect the power supply cable to the IRFU (Figure 93). Check that the power connector screws are tight enough to hold the power cable securely in place.

> **NOTE**
> For EMI Class B compliance, a 10 AWG braided shielded power cable with drain wire and foil is recommended.

If a battery is being used to supply power, connect the ‘common’ battery terminal to the main electrical grounding system (not directly to the building grounding system).

Figure 93 IRFU power connection



Installing the CMU

This section describes how to mount the CMU in the building or cabinet, and to connect it to ground, power supply and PC.

When installing a 1+1 Hot Standby link, install two CMUs at each end, one for the Primary and one for the Secondary unit.

When installing a 2+0 link, install two CMUs at each end, one for the link 'A' and one for the link 'B' ODU.

⚠ CAUTION

To minimise radiated emissions, use screened Ethernet cable for all copper connections from the CMU Ethernet ports. This includes the Data port connection to any network switch and the Management port to the splitter WB3807 (if fitted) and onwards to any network switch.

Maximum operating ambient temperature for the CMU

⚠ WARNING

HOT SURFACES: care should be taken when handling an operating CMU.

Mount the CMU on either a horizontal or vertical surface using the supplied mounting bracket. Do not operate the CMU in ambient temperatures exceeding 40 deg C unless mounted in a Restricted Access Location.

At ambient temperatures over this limit, the temperature of the external metal case parts of the CMU may exceed a touch temperature of 70 deg C. Heat warning labels are fixed adjacent to the hottest parts, on the top of the unit adjacent to the rear face and to the front panel mounted N type connector.

Operation of CMU in a Restricted Access Location

The CMU may be operated in ambient temperatures up to 55°C when it is housed in a Restricted Access Location. Under these conditions the temperature of the external metal case parts of the CMU may exceed a touch temperature of 70°C, but will be less than 90°C.

A Restricted Access Location is defined (in EN 90650-1) as one where access may only be gained by use of a tool or lock and key, or other means of security, and access is controlled by the authority responsible for the location.

Examples of permissible Restricted Access Locations are:-

- A lockable equipment room.
- A lockable cabinet.

Access must only be gained by persons who have been instructed about the reasons for the restrictions applied to the location and about any precautions that must be taken.

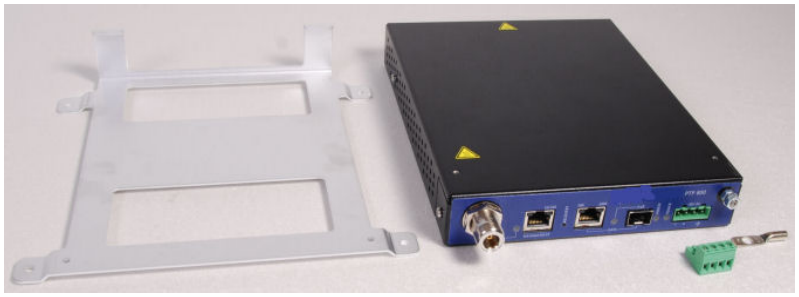
Mounting the CMU

Mount the CMU in one of three ways:

- On a shelf or bench top.
- On a wall.
- In a cabinet rack.

The CMU kit contains the CMU, CMU bracket, power connector and ground lug (Figure 94).

Figure 94 CMU kit contents



⚠ CAUTION

To prevent the CMU from overheating, ensure that the ventilation holes on the side of the CMU are not obstructed and that there is room for air flow across the back of the CMU (the end opposite the connector face).

Shelf or bench top mounting

When mounting on a shelf or bench top (Figure 95), secure the CMU using its bracket. The bracket screws to the base of the CMU.

Figure 95 CMU mounted on bench



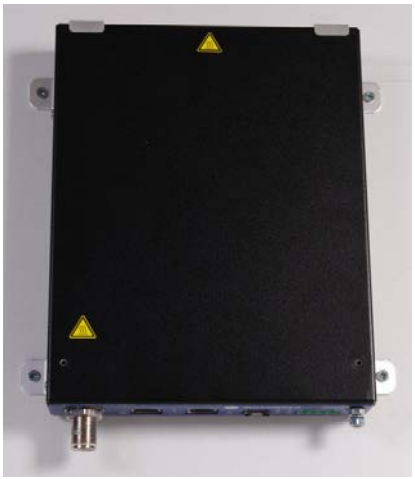
Wall mounting

When mounting on a wall (Figure 96), secure the CMU using its bracket. To allow fixing holes to be made, place the bracket against the wall, then secure the bracket to the CMU using the screws supplied, before offering the assembly up to the wall for fixing.

⚠ WARNING

In order to comply with safety certification, mount the CMU with the connectors facing upwards or downwards; do not mount the CMU with the connectors facing sideways.

Figure 96 CMU mounted with bracket



Rack mounting

When moutning in a 19 inch cabinet rack, use a rack mounting kit (Figure 97 and Figure 98). This can be used for one or two CMUs. The kit contains a blanking plate and CMU securing screws.

Figure 97 CMU with rack mounting kit and blanking plate



Figure 98 CMU mounted in rack



CAUTION

To avoid damaging the RF cable, route it in such a way that the minimum bend radius for the selected cable is always exceeded.

If cables are laid in an air-handling cavity, they must be Plenum rated.

Grounding the CMU

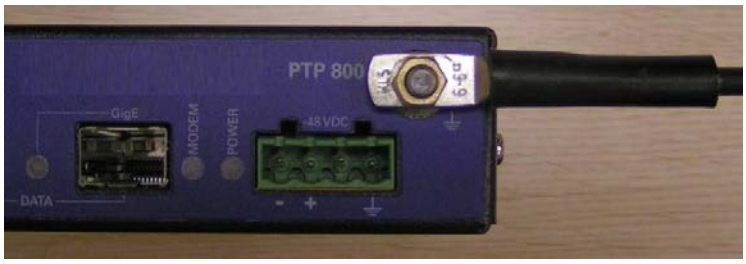
Ground the CMU to a rack ground bar, master ground bar or other suitable ground using a minimum cable cross section of 10 mm^2 (6AWG) (Figure 43). It is a condition of the safety approval that the unit is grounded.

NOTE

For a 1+1 Hot Standby link, ground both CMUs to the same grounding point (Figure 44).

Attach the ground cable to the CMU ground connector (Figure 99).

Figure 99 CMU ground connector



Connecting the CMU to the IF cable

> **NOTE**
> If space inside the cabinet is limited, install a right angle IF cable connector (Cambium part number 01010589001) (Figure 100).

Figure 100 Rack mounted CMU with a right angled IF cable connector



ODU-based deployments

Cut any surplus length from the CMU end of the ODU-CMU IF cable and fit an N type connector, as described in Fitting an N type connector to an IF cable on page 5-38. Connect this IF cable to the CMU.

For 1+1 and 2+0 links, repeat for the second ODU and CMU.

NOTE

For an ODU-based 1+1 Hot Standby link with an asymmetric coupler, make the following connections:

1) Connect the IF cable from the 'MAIN' side of the ODU coupler to the CMU labelled 'Primary'.

2) Connect the IF cable from the 'STANDBY' side of the ODU coupler to the CMU labelled 'Secondary'.

IRFU-based deployments

Connect the supplied IF cable (Cambium part number 30009403001) to the CMU.

For 1+1 and 2+0 links, repeat for the second transceiver unit and CMU.

NOTE

For an IRFU-based 1+1 Hot Standby link with the unequal coupling option, make the following connections:

1) Connect the IF cable from the primary (left hand) transceiver to the CMU labelled 'Primary'.

2) Connect the IF cable from the secondary (right hand) transceiver to the CMU labelled 'Secondary'.

Connecting the CMU power supply

Connect the CMU to a minus 48 Volt (−48V) supply capable of supplying a maximum of 2 amps.

The Cambium supplied AC to DC converter is shown in Figure 101. For specifications of the converter, mains cables and DC connectors, refer to AC to DC converter specifications on page 4-4.

Figure 101 Cambium AC to DC converter



For details of alternative power supply arrangements, refer to Power supply considerations on page 2-4. If an alternative power supply is to be installed, ensure that it meets the following safeguards:

- The DC supply has over current protection that does not exceed 3 amps
- There is a way to isolate the CMU from the DC supply.

If a DC connector has to be attached to the DC output cable, use the following pin connections:

- Pin 1: −48 Volts
- Pin 2: 0 Volts
- Pin 3: Not Connected
- Pin 4: Chassis ground

Pin 1 is the left most pin on the CMU power connector when looking at the front panel.

Preparing network connections (1+0 and 2+0 links)

This section describes how to prepare the cables to connect the CMU to router ports, switch ports or other equipment in the customer and (optionally) management networks. It applies only to unprotected ends (1+0 and 2+0 links).

When installing a 2+0 link, prepare separate network connections for the link ‘A’ and the link ‘B’ CMUs.

> **NOTE**
> The CMU is not normally connected to the network equipment until antenna alignment is complete (as described in Task 15: Connecting link to the network on page 6-114).

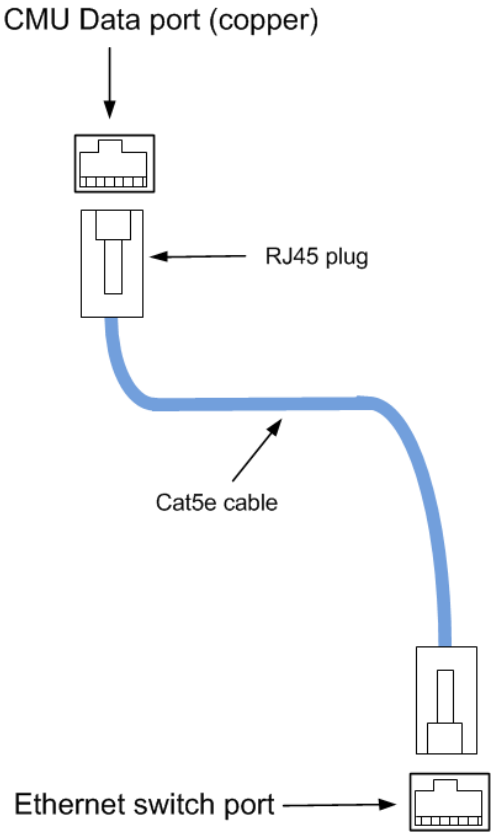
For all management modes (out-of-band and in-band), decide whether the data network connection is to be copper or fiber, then perform either Installing a copper data interface on page 5-85 or Installing a fiber data interface on page 5-86.

For out-of-band management modes (but not in-band), perform Installing a management interface on page 5-87.

Installing a copper data interface

If an unprotected configuration requires a copper data interface, connect the CMU Data port (copper) to the network as shown in Figure 102.

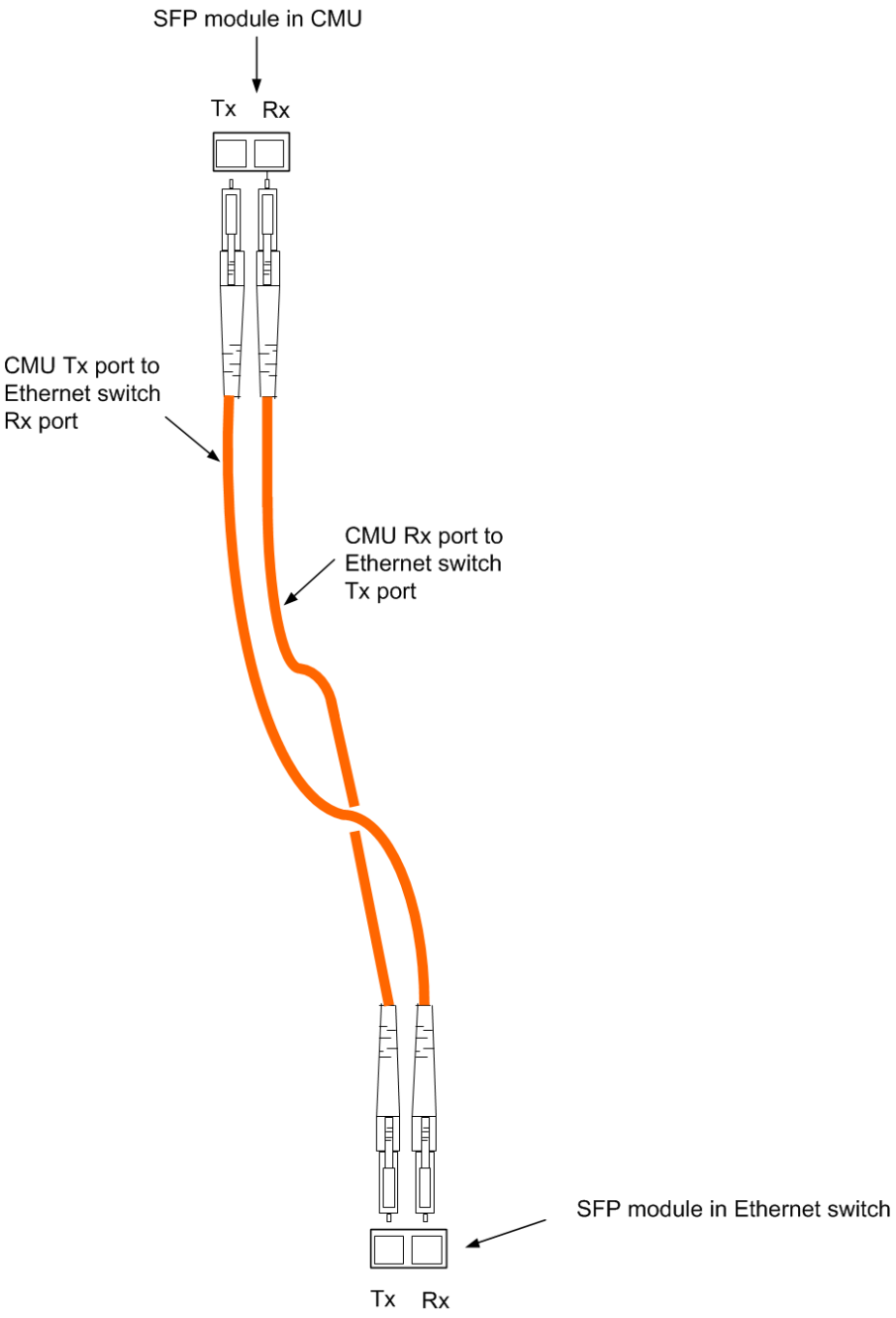
Figure 102 Copper data interface connections



Installing a fiber data interface

If an unprotected configuration requires a fiber data interface, connect the CMU Fiber SFP (GigE) port to the network as shown in Figure 103.

Figure 103 Fiber data interface connections



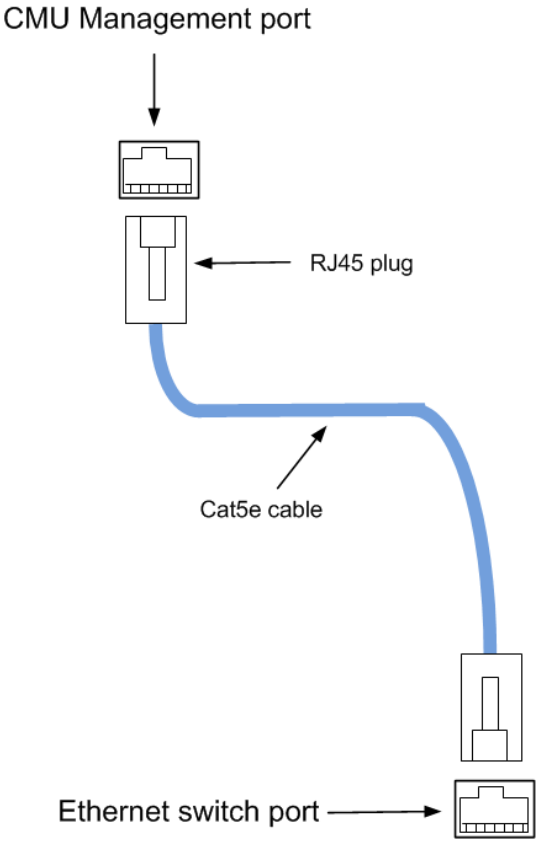
Refer to Connecting fiber cables to the CMU on page 5-88.

Installing a management interface

If an unprotected configuration requires a management interface, connect the CMU Management port to the network as shown in Figure 104.

> **NOTE**
> At the edge of a network, if the management network equipment is inaccessible, leave the CMU management port disconnected.

Figure 104 Management interface connections



Connecting fiber cables to the CMU

To connect fiber cables to the CMU, proceed as follows:

1. Insert an SFP module into the GigE port of the CMU with the PCB connector down and label up.



2. Remove the protective caps from the LC connectors.



3. Plug the LC connectors into the SFP module, ensuring they snap home.



Preparing network connections (1+1 Hot Standby)

This section describes how to prepare the cables to connect the CMU to the Ethernet switch in the customer and (optionally) management networks. It applies only to protected ends (1+1 Hot Standby links).

> **NOTE**
> The CMU is not normally connected to the network equipment until antenna alignment is complete. See Task 15: Connecting link to the network on page 6-114.

Select and install the required interfaces depending on the choice of management mode and network connection (Table 218).

Table 218 Selecting network interfaces for 1+1 Hot Standby links

Management mode	Network connection	Procedures
Out-of-band (Figure 59)	Customer data	Either: Installing a redundant copper interface on page 5-91; Or: Installing a redundant fiber interface on page 5-92; Or: one copper and one fiber (*1); Or: Installing a Fiber-Y interface on page 5-93.
	Management data (not 'last hop')	Installing an out-of-band protection splitter on page 5-90
	Management data ('last hop') (*2)	Either: Installing an out-of-band protection splitter on page 5-90, but connect the two LAN ports together using a protection cable; Or: Installing a protection cable on page 5-94.
In-band (Figure 61)	Customer data	Either: Installing a redundant copper interface on page 5-91; Or: Installing a redundant fiber interface on page 5-92; Or: one copper and one fiber (*1).
	Management data	Installing a protection cable on page 5-94

(*1) It is possible to combine the two types of redundant interface at one link end, that is, connect one CMU to the network via copper and the other CMU via fiber.

(*2) 'Last hop' link ends are those that are at the edge of the network, where access to the management network is not always available.

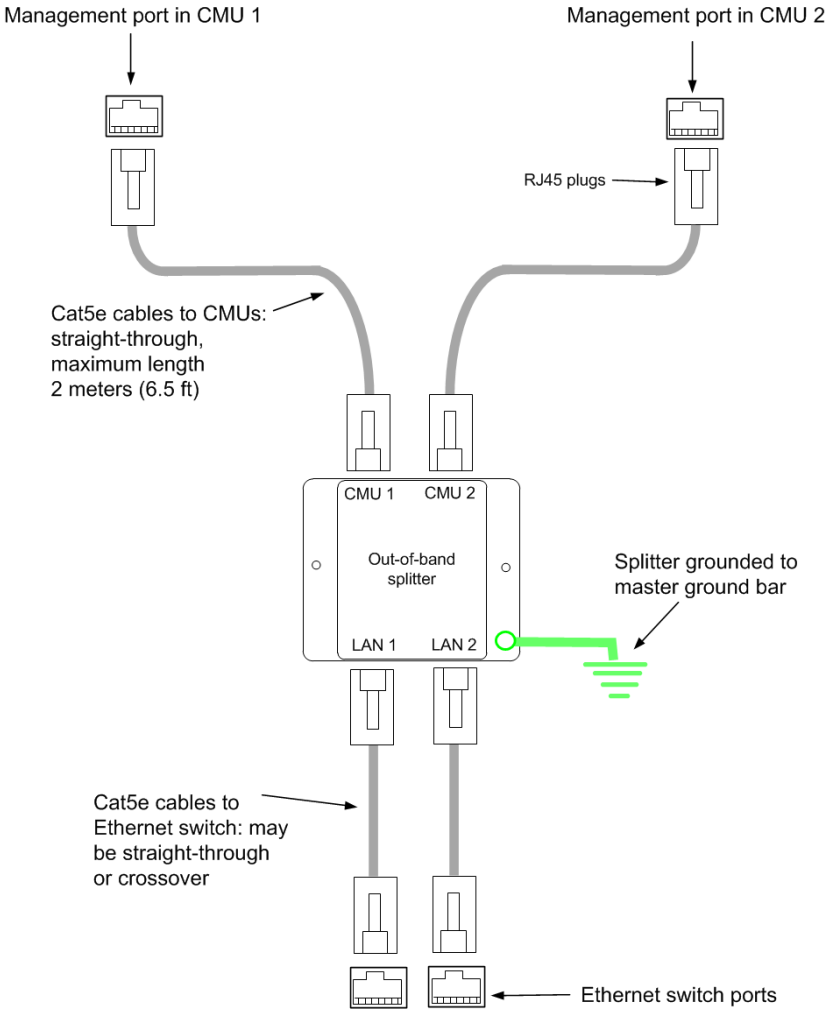
Installing an out-of-band protection splitter

If a 1+1 protected configuration requires an out-of-band protection splitter, connect the CMU Management ports to the management network as shown in Figure 105.

Use straight-through Cat5e cables with a maximum length of 2 m to connect the CMUs to the splitter.

> **NOTE**
> At the edge of the network (the 'last hop'), if no management network equipment is available, the two LAN ports can be connected using a protection cable. The cable pin outs are specified in Protection cable on page 4-17.

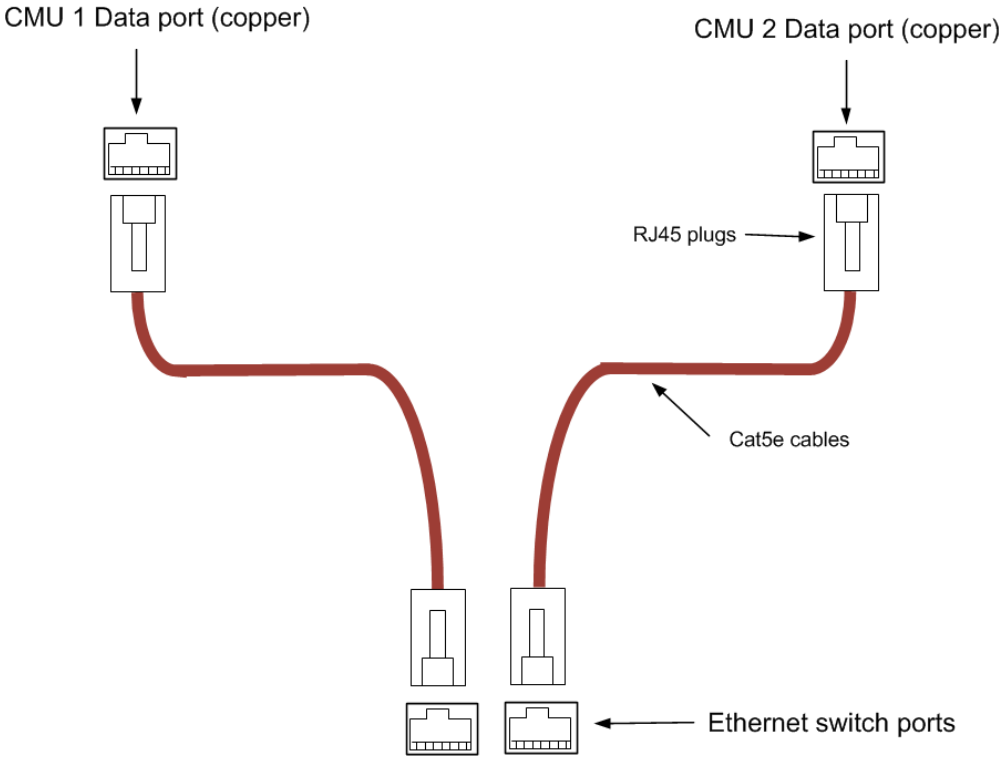
Figure 105 Out-of-band protection splitter connections


Management port in CMU 1
Management port in CMU 2
RJ45 plugs
Cat5e cables to CMUs: straight-through, maximum length 2 meters (6.5 ft)
CMU 1
CMU 2
Out-of-band splitter
LAN 1
LAN 2
Splitter grounded to master ground bar
Cat5e cables to Ethernet switch: may be straight-through or crossover
Ethernet switch ports

Installing a redundant copper interface

If a 1+1 protected configuration requires a redundant copper interface, connect the CMU Data ports (copper) to the network as shown in Figure 106.

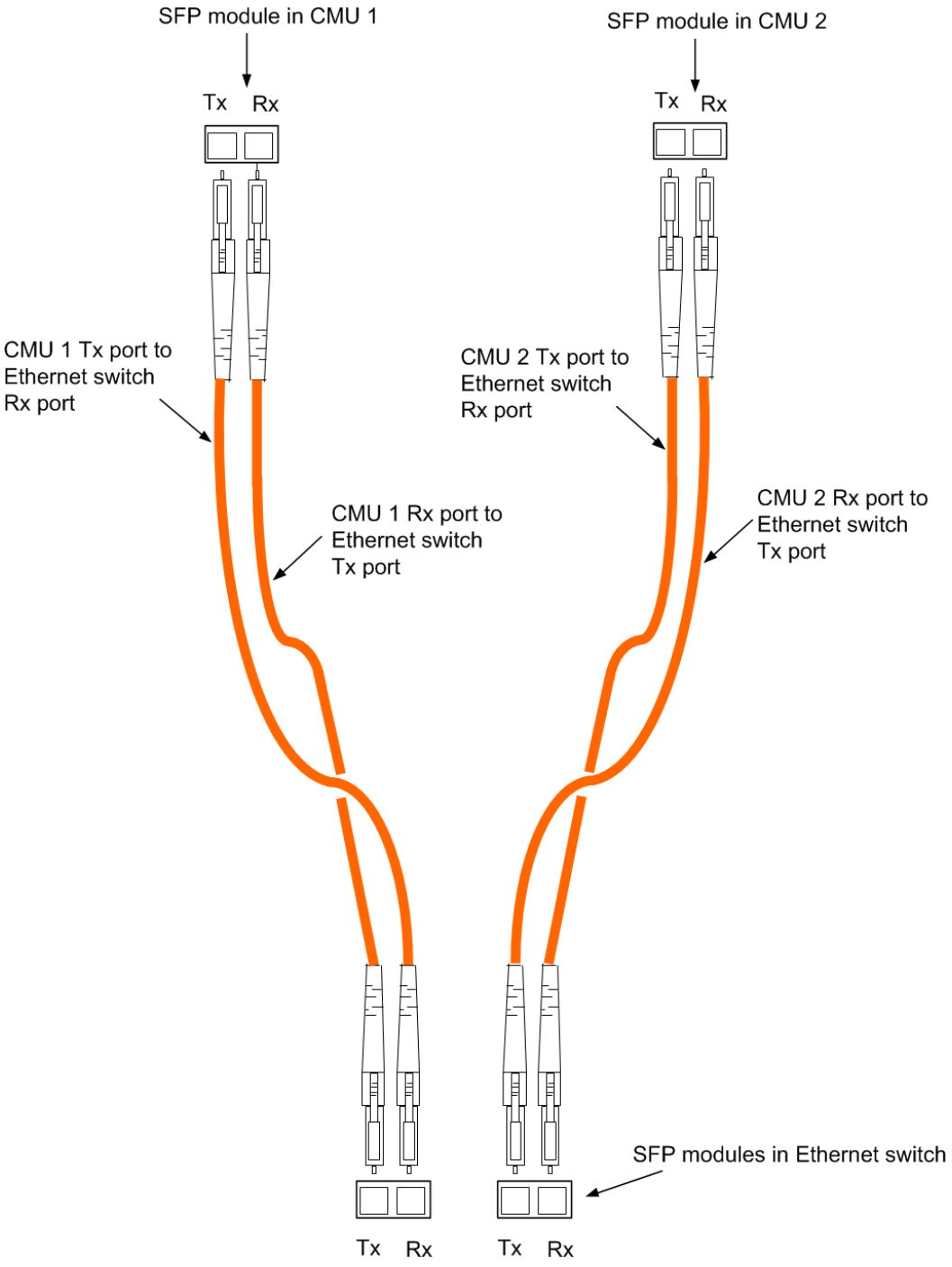
Figure 106 Redundant copper interface connections



Installing a redundant fiber interface

If a 1+1 protected configuration requires a redundant fiber interface, connect the CMU Fiber SFP (GigE) ports to the network as shown in Figure 107.

Figure 107 Redundant fiber interface connections

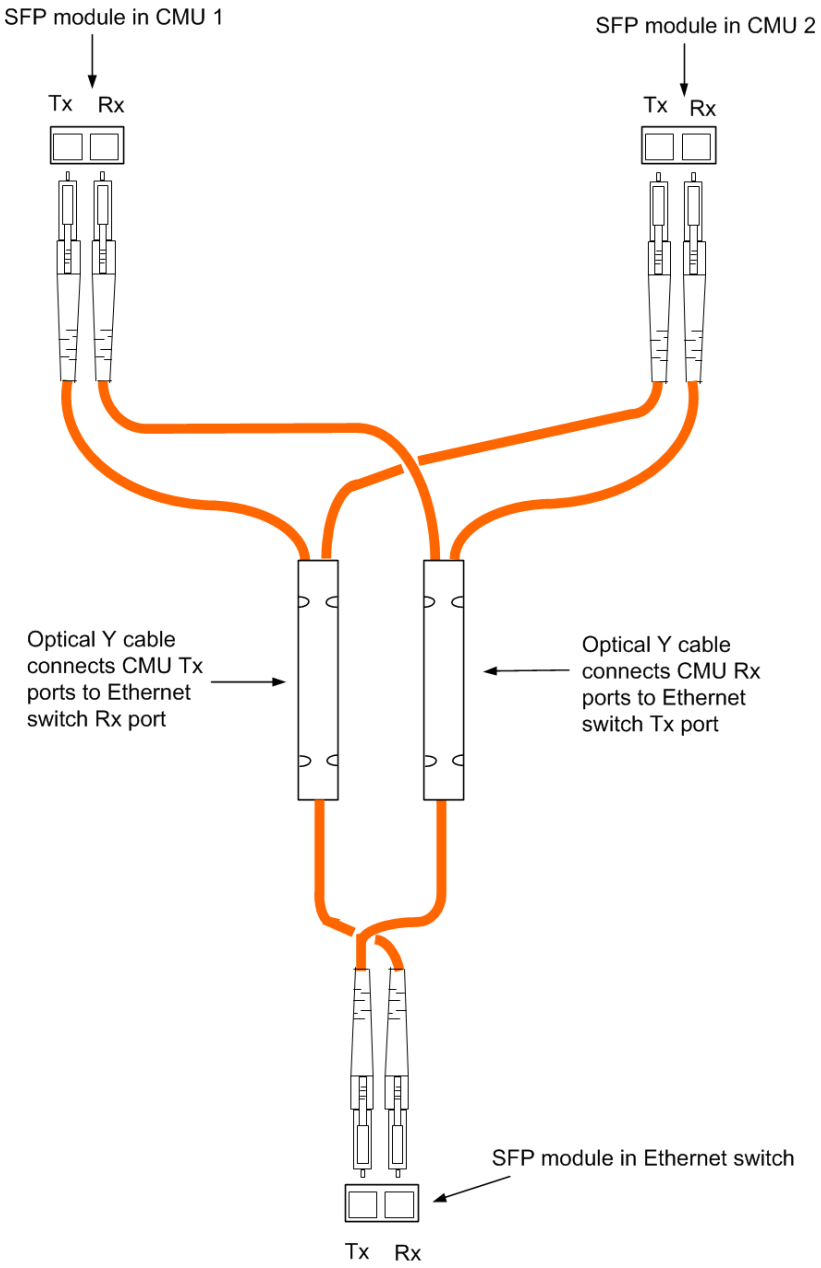

SFP module in CMU 1
SFP module in CMU 2
Tx Rx
Tx Rx
CMU 1 Tx port to Ethernet switch Rx port
CMU 2 Tx port to Ethernet switch Rx port
CMU 1 Rx port to Ethernet switch Tx port
CMU 2 Rx port to Ethernet switch Tx port
SFP modules in Ethernet switch
Tx Rx
Tx Rx

Refer to Connecting fiber cables to the CMU on page 5-88.

Installing a Fiber-Y interface

If a 1+1 protected configuration requires a Fiber-Y interface, connect the CMU Fiber SFP (GigE) to the customer network as shown in Figure 108.

Figure 108 Optical Y interface connections


SFP module in CMU 1
Tx Rx
SFP module in CMU 2
Tx Rx
Optical Y cable connects CMU Tx ports to Ethernet switch Rx port
Optical Y cable connects CMU Rx ports to Ethernet switch Tx port
SFP module in Ethernet switch
Tx Rx

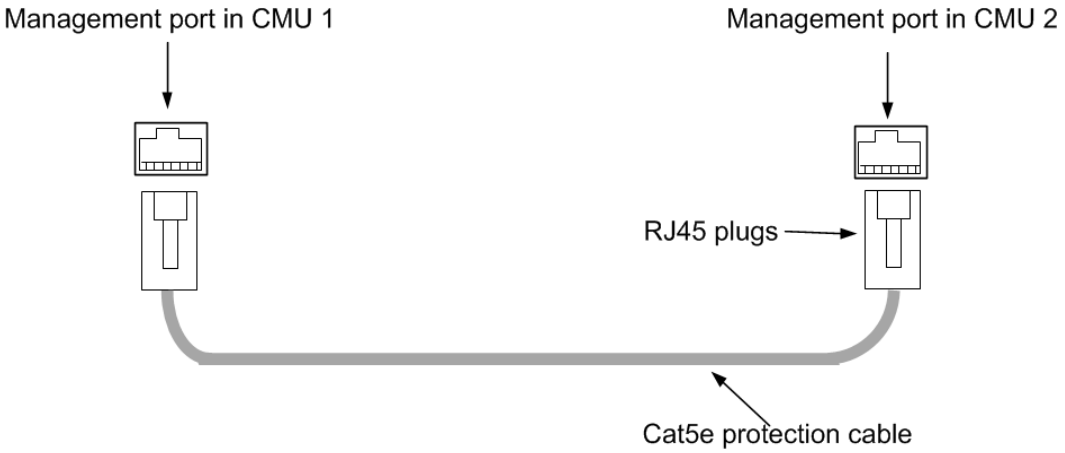
Refer to Connecting fiber cables to the CMU on page 5-88.

Installing a protection cable

If a 1+1 protected configuration requires a protection cable, connect the CMU Management ports together as shown in Figure 109.

The cable pin outs are specified in Protection cable on page 4-17.

Figure 109 Protection cable connections



Replacing IRFU components

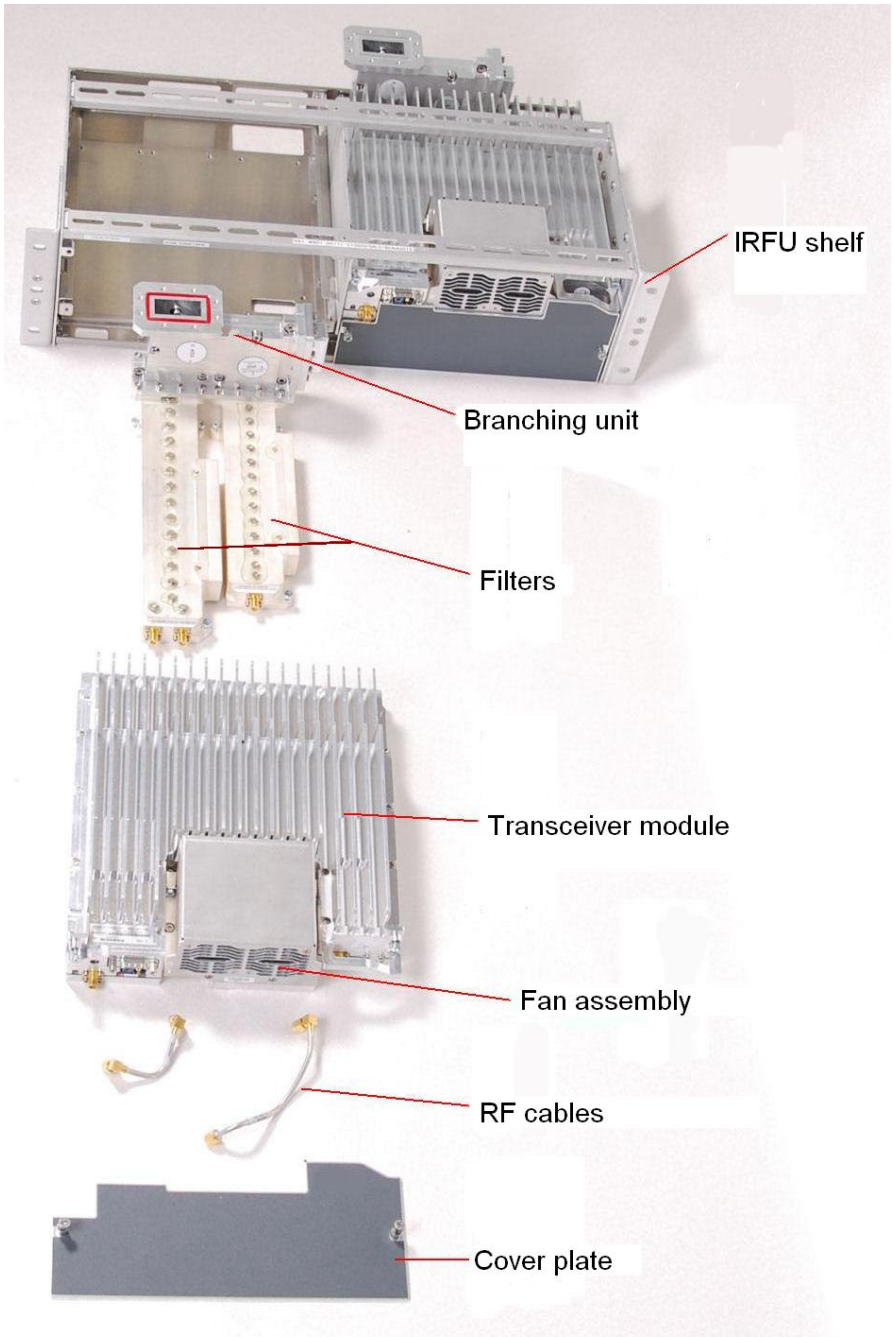
NOTE
Applies to IRFU deployments only.

Perform this task to replace IRFU components in the field (Figure 110).

CAUTION
Before removing or replacing a main component, wear an ESD wrist strap and attach its free end (or clamp) to the grounding lug of the IRFU.

NOTE
IRFUs ship fully assembled per customer's ordered options. Figure 110 identifies all field-replaceable parts.

Figure 110 IRFU components (example)



Before replacing IRFU components, check that the required tools are available (Table 219).

Table 219 Tools required for IRFU component replacement

Item	Required specifications	Where used
Screwdriver	Phillips #1, small tip	For installing a fan assembly
Screwdriver	Phillips #2, medium tip	Throughout
Ball-point allen key	7/64	For installing filters
Open-end wrench	5/16	For installing a transceiver and RF cable
SMA torque wrench w/right-angle adaptor	Model ST-SMA8, (from Fairview Microwave Inc.)	
Standard torque wrench	5/16, set to 0.1 kg•m (9.0 lb-inch)	

Replacing a transceiver

When replacing a transceiver, refer to Figure 111.

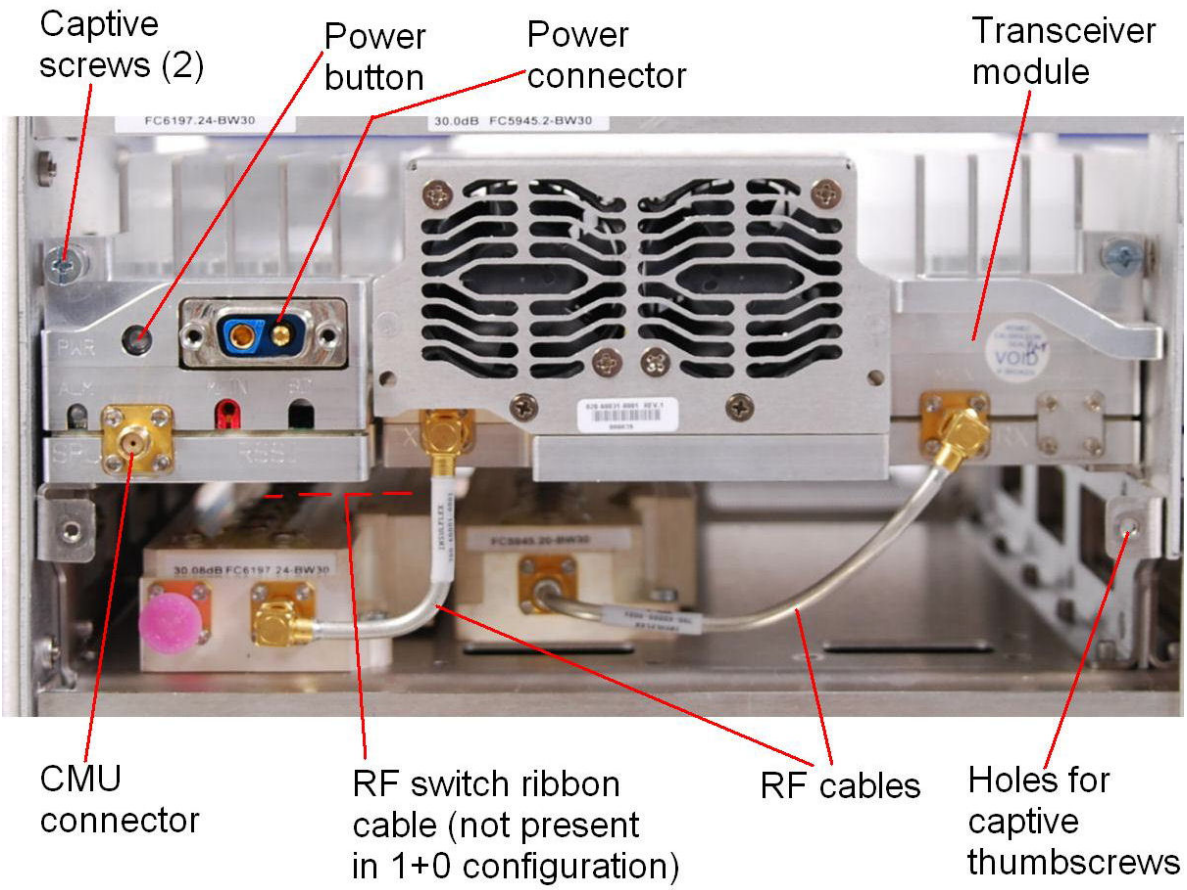
CAUTION

In an unprotected link, this procedure will affect traffic. In a 1+1 Hot Standby link, ensure that traffic is locked on the available channel during maintenance.

NOTE

Ensure that the new transceiver has the same part number as the discarded one.

Figure 111 Transceiver replacement (1+0 example)



Remove the transceiver

To remove the old transceiver, proceed as follows:

1. Power off the CMU.
2. Push the PWR button OFF for at least 3 seconds, until the PWR LED is Off.

> **NOTE**
> This ensures that there are no sparks at the DC power connectors when removing DC from the transceiver. This will also indicate to the IRFU controller that, after installing the new transceiver, the PWR button has to be pushed ON again. Otherwise, power will automatically turn on when DC power is reconnected to the newly installed transmitter.

3. Disconnect both the power cable and IF cable from their respective connectors on the IRFU.

4 Remove the IRFU section Cover Plate by unfastening both its Captive thumbscrews.

5 Disconnect all RF cables from the transceiver, and the RF switch ribbon cable (not present in 1+0 configurations) from the bottom of the transceiver.

> **NOTE**
> To reduce replacement time, it may be more practical to disconnect only the end of each cable from the transceiver, and leave all cables within the shelf, provided they do not interfere with the removal and installation of the transceiver.

6 Unfasten the transceiver captive Captive screws (2), then carefully slide the Transceiver module out of the shelf. It might be necessary to slightly raise the transceiver in the front as it is being slid out.

Install the new transceiver

To install the new transceiver, proceed as follows:

1 Connect the RF switch ribbon cable (not present in 1+0 configurations) to the bottom of the new transceiver.

2 Space permitting, use the Standard torque wrench set to 0.1 kg-m (9.0 lb-inch) to tighten each connector nut. Otherwise, use the SMA torque wrench w/right-angle adaptor to tighten the SMA connectors.

3 As an alternative, first hand-tighten the RF cable connector nuts to the transceiver ports, slide the transceiver in the shelf, then fasten its Captive screws (2) to secure it in place.

4 As appropriate, use the Standard torque wrench or the SMA torque wrench w/right-angle adaptor, set to 0.1 kg•m (9.0 lb-inch), to tighten all RF cable connector nuts.

5 Replace the IRFU section cover plate by fastening both its Captive thumbscrews.

6 Connect both the Power cable and Coaxial cable to their respective connectors on the IRFU.

7 Push the PWR button ON.

Once the radio link is re-established, verify that there are no alarms.

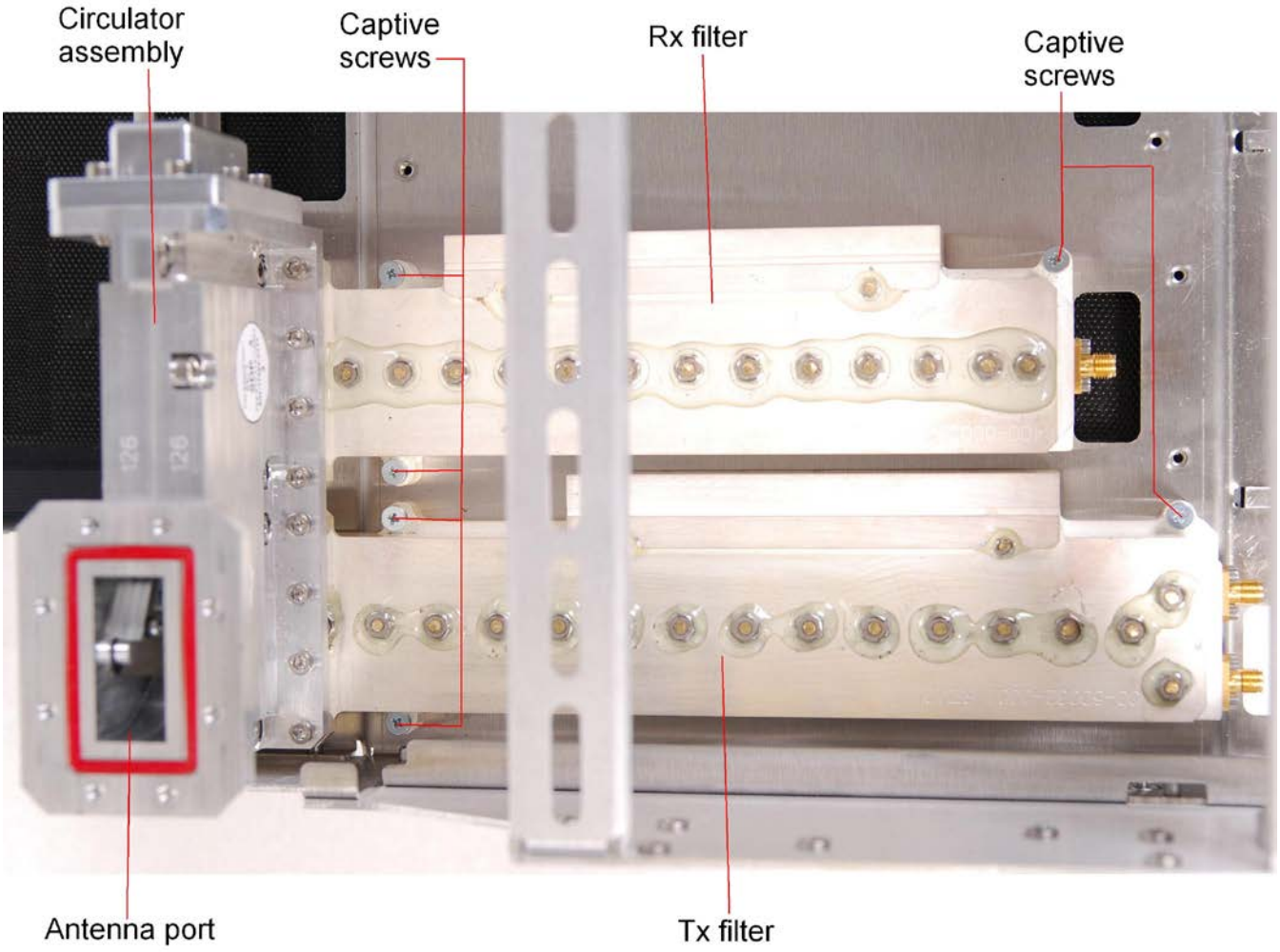
Replacing a branching unit

When replacing a branching unit, refer to Figure 112.

⚠ CAUTION

This procedure will interrupt traffic, whether the system is protected or non-protected.

Figure 112 Branching unit replacement



Remove the branching unit

To remove the old branching unit, proceed as follows:

1. Disconnect any flexible waveguide(s) from the Antenna Port(s).
2. Remove the Transceiver, following the procedure Remove the transceiver on page 5-98.

3. Remove the cable between the Tx filter to the RF switch.
4. Unfasten the six Captive screws attaching the Tx Filter and the Rx Filter to the bottom of the shelf. Refer to Figure 112 for locating the screws.
5. Remove the BU Assembly (filters and Circulator Assembly) from the shelf.

Install the new branching unit

To install the new branching unit, proceed as follows:

1. Assemble the BU. Reuse disassembled components only if they are sound. Use new components bearing the same specifications as the original ones.
2. Position the replacement BU Assembly in its designated location, ensuring to align properly all screws on the filters with their corresponding holes on the bottom of the shelf.
3. Re-fasten the 6 Captive screws unfastened earlier, to secure the BU Assembly to the bottom of the shelf. DO NOT overtighten.

Reinstall the transceiver

To reinstall the transceiver after replacing the branching unit, proceed as follows:

1. Reconnect the RF switch ribbon cable to the bottom of the transceiver, slide the transceiver in the shelf, then fasten its Captive screws (2) to secure it in place.
2. Using a 5/16 inch SMA torque wrench w/right-angle adaptor or a Standard torque wrench set to 0.1 kg•m (9.0 lb-inch), reconnect the RF cables to the transceiver, referring to the applicable configuration. For guidance, follow procedure Install the new RF cable on page 5-105.
3. Re-place the IRFU section cover plate by fastening both its Captive thumbscrews.
4. Connect both the Power cable and Coaxial cable to their respective connectors on the IRFU.
5. Push the PWR button ON.

   Once the radio link is re-established, verify that there are no alarms.

Replacing filters

When replacing filters, refer to Figure 113.

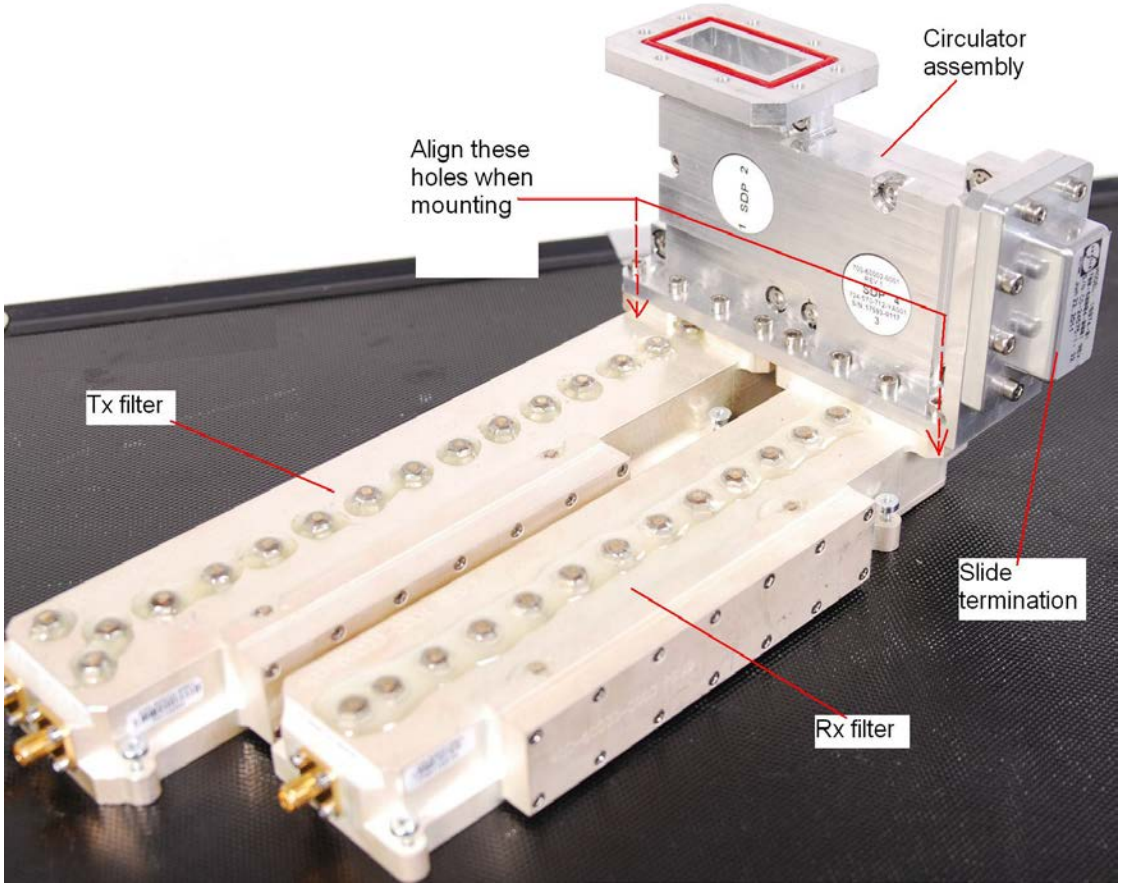
NOTE

This step is only required when changing frequencies, without changing bands. However, to facilitate the removal of filters, perform Remove the branching unit on page 5-100.

CAUTION

This procedure will interrupt traffic, whether the system is protected or non-protected.

Figure 113 Filter replacement



Remove the filters

1. Perform Remove the branching unit on page 5-100.
2. Deposit the BU (Circulator an filters assembly) on a flat surface.
3. Unfasten all required socket-head screws, and keep them for reuse.

4 Separate the Circulator Assembly from both filters.

Install new filters

1 Refer to Figure 113 for aligning the outside corners and screw holes of the Circulator Assembly and the Filter flanges.

2 Insert and hand tighten each socket-head screw in its respective hole, taking care not force or rip the screw threads.

3 Secure all screws, using the Ball-point Allen key, without overtightening.

4 Follow Steps 2 and 3 from procedure Install the new branching unit on page 5-101.

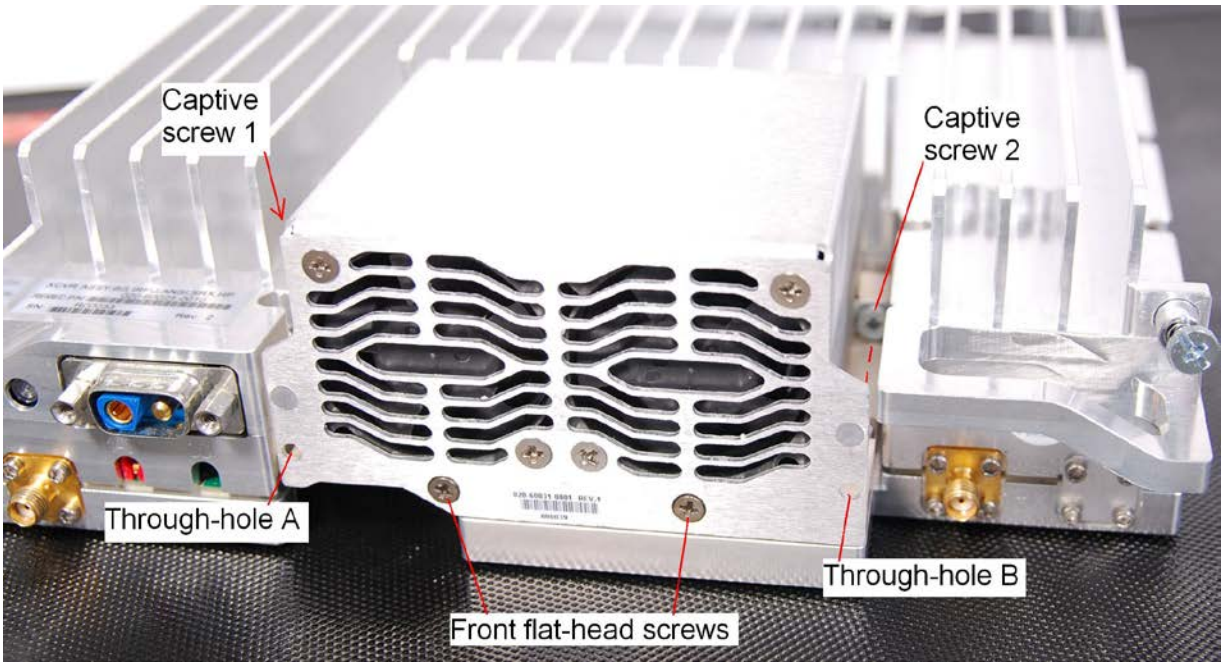
Replacing a fan assembly

When replacing a fan assembly, refer to Figure 114.

⚠ WARNING

If replacing a fan assembly while the radio is operating, complete this procedure as quickly as possible, otherwise the unit may overheat. Surface may be hot to touch.

Figure 114 Fan assembly replacement



Remove the fan assembly

To remove the old fan assembly, proceed as follows:

1. Unfasten the two front flat-head screws (#4-40), and keep them for re-use.
2. Insert a Phillips small-tip screwdriver in Through-holes A and B to reach and unfasten the two Captive screws 1 and 2.
3. Once Captive screws 1 and 2 are completely unfastened, grasp the Fan Assembly by its sides, pull it forward and disconnect cables, then pull it out of the shelf.

Install the new fan assembly

To install the new fan assembly, proceed as follows:

1. Place the fan assembly over the transceiver, making sure to properly align Captive screws 1 and 2 with their respective screw holes.
2. Connect the cables; then, using a Phillips small-tip screwdriver inserted through holes A and B, fasten Captive screws 1 and 2.
3. Fasten the two Front flat-head screws. Carefully observe connector keying.

Replacing an RF cable

When replacing RF cables, refer to Figure 115 and Table 220 as a guide for connecting each cable, using the appropriate connector (angled or straight) to the corresponding component.

Figure 115 RF cable installation and removal (1+1 Tx MHSB / Rx SD example)

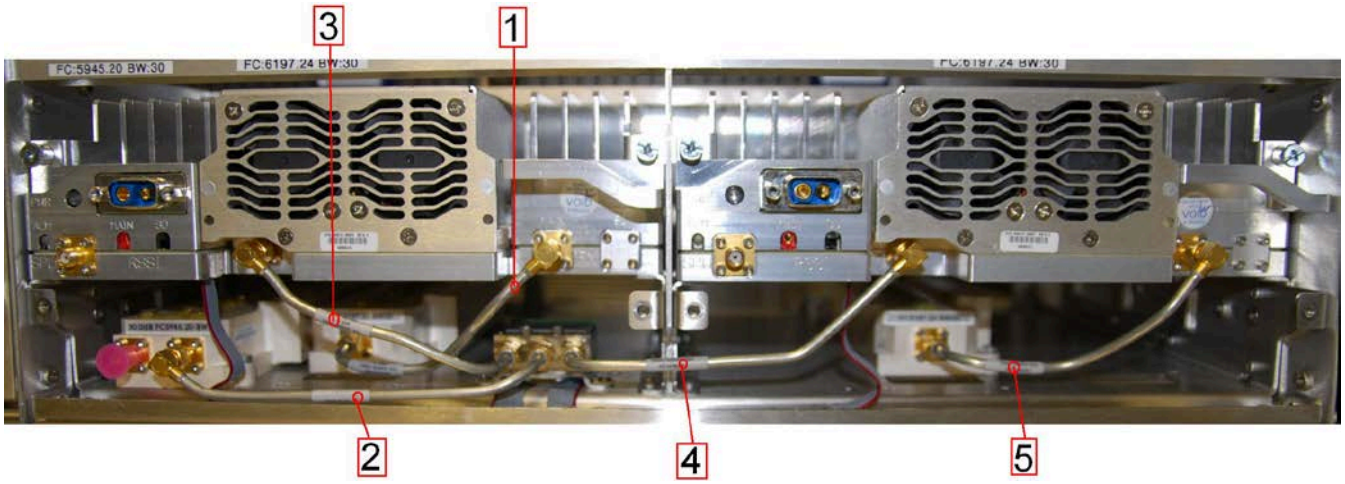


Table 220 RF cable connections (1+1 Tx MHSB / Rx SD example)

#	Part number	SMA cable connector from (angled)	SMA cable connector to (straight)
1	30009399001	Transceiver A	Rx Filter A
2	30009399004	Tx Filter A	RF Switch
3	30009399005	Transceiver A	RF Switch
4	30009399006	Transceiver B	RF Switch
5	30009399001	Transceiver B	Rx Filter B

Remove the RF cable

To remove an RF cable, proceed as follows:

1. Note the Part Number printed on the label of the cable before removal, referring to Table 220 as an example.
2. Using the Standard torque wrench or SMA torque wrench w/right-angle adaptor, unscrew each connector's end nut for about three 1/4 turns, enough to reduce resistance, then continue by hand until free.

Install the new RF cable

To install an RF cable, proceed as follows:

1. Before installing the replacement RF cable, verify that its Part Number matches exactly that of the discarded cable.
2. Fastening each cable-end nut by hand, start with the angled connector, then follow by the straight one, as identified in Table 220.
3. Space permitting, use the Standard torque wrench set to 0.1 kg•m (9.0 lb-inch) to tighten each connector nut. Otherwise, use the SMA torque wrench w/right-angle adaptor to tighten the SMA connectors.
4. As an alternative, first hand-tighten the RF cable connector nuts to the transceiver ports – referring to the applicable configuration from IRFU configuration options on page 1-20 – slide the transceiver in the shelf, then fasten its Captive screws (2) to secure it in place.
5. As appropriate, use the Standard torque wrench or the SMA torque wrench w/right-angle adaptor, set to 0.1 kg•m (9.0 lb-inch), to tighten all RF cable connector nuts.

Chapter 6: Configuration and alignment

This chapter describes how to configure a PTP 800 link and align its antennas.

Observe the precautions in Preparing for configuration and alignment on page 6-2.

Configure the two units by performing the following tasks:

- Task 1: Connecting to the unit on page 6-3
- Task 2: Configuring IP and Ethernet interfaces on page 6-8
- Task 3: Installing license keys on page 6-21
- Task 4: Upgrading software version on page 6-25
- Task 5: Configuring security on page 6-28
- Task 6: Configuring protection on page 6-53
- Task 7: Configuring wireless interface on page 6-63
- Task 8: Setting up SNMP agent on page 6-77
- Task 9: Configuring alarms and messages on page 6-90
- Task 10: Configuring syslog on page 6-94
- Task 11: Configuring remote access on page 6-96

When all equipment has been installed at both link ends, perform the following tasks:

- Task 12: Aligning antennas on page 6-98
- Task 13: Reviewing configuration and performance on page 6-106
- Task 14: Configuring quality of service on page 6-111
- Task 15: Connecting link to the network on page 6-114

NOTE

If FIPS 140-2 secure mode is required, refer to Configuring for FIPS 140-2 applications on page 6-121.

NOTE

For 1+1 Hot Standby links, configure all four units and align all antennas.

Preparing for configuration and alignment

Before proceeding with unit configuration and antenna alignment, perform the checks described in this section.

Safety precautions during configuration and alignment

All national and local safety standards must be followed while configuring the units and aligning the antennas.

⚠ WARNING

Ensure that personnel are not exposed to unsafe levels of RF energy. The units start to radiate as soon as they are powered up. Respect the safety standards defined in Radiation hazard assessment on page 4-86, in particular the minimum separation distances.

Observe the following guidelines:

- Never work in front of the antenna when the CMU is powered.
- Always power down the CMU before connecting or disconnecting the drop cable from the CMU, RFU or LPU.

Regulatory compliance during configuration and alignment

When configuring the units and aligning the antennas, follow all applicable radio regulations. For more information, refer to Electromagnetic compliance on page 4-82.

⚠ CAUTION

USA only: if the system designer has provided a list of channels to be barred for TDWR radar avoidance, bar the affected channels during staging, before the units are allowed to radiate on site, otherwise FCC rules will be infringed.

Selecting configuration options

Use the installation report to determine which configuration options are required. Refer to Link planning on page 2-2.

Task 1: Connecting to the unit

This task consists of the following procedures:

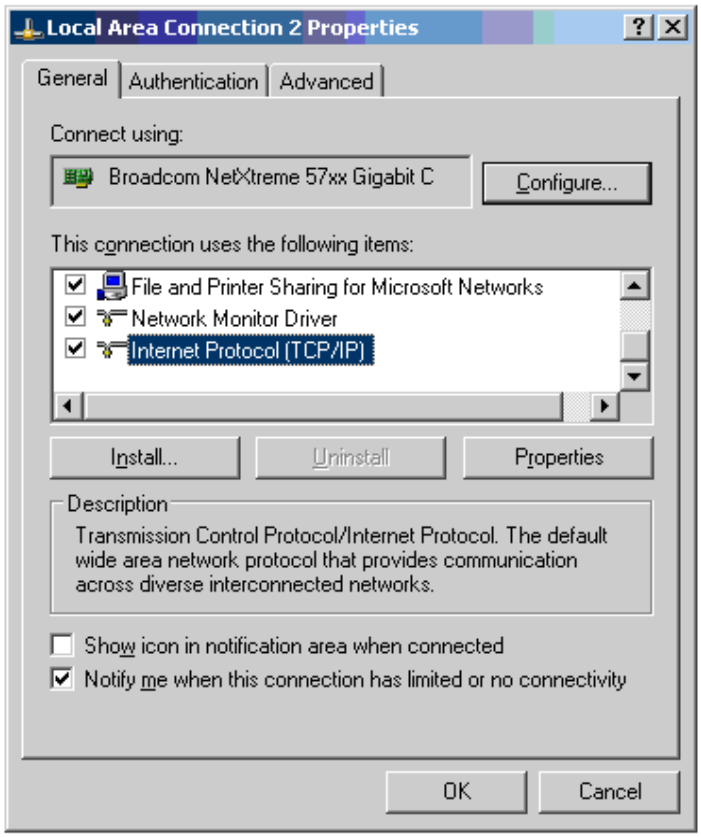
- Configuring the management PC on page 6-3
- Updating the ARP table on page 6-5
- Connecting to the PC and powering up on page 6-6
- Logging into the web interface on page 6-6

Configuring the management PC

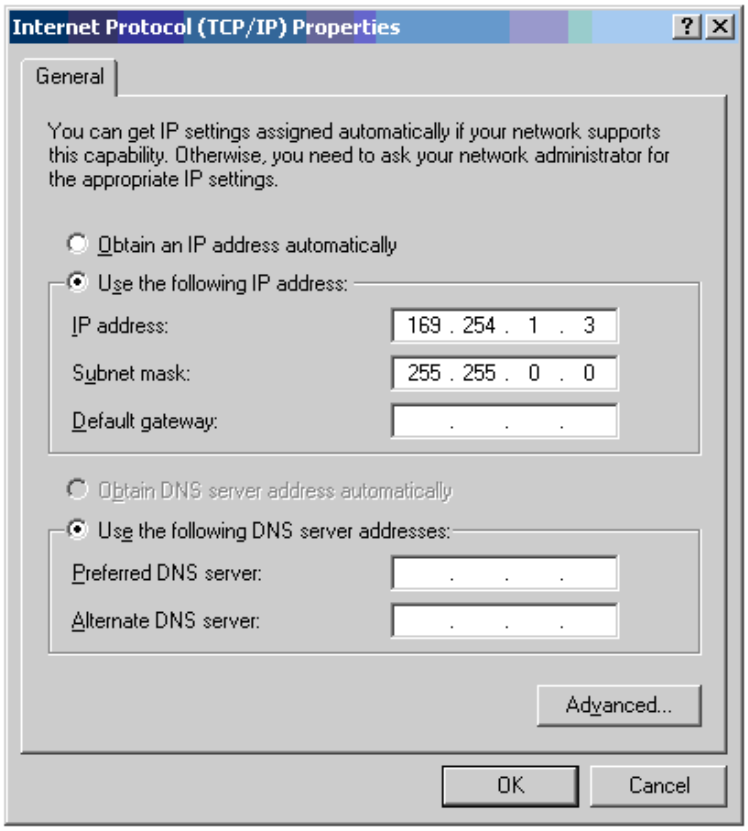
To configure the local management PC to communicate with the PTP 800, proceed as follows:

1 Display the Local Area Connection Properties dialog.

The path to this dialog depends on Windows version and PC configuration, for example select: **Control Panel, Network Connections, Local Area Connection, Properties**.



2 Select Internet Protocol (TCP/IP) and click on **Properties**. The Internet Protocol (TCP/IP) Properties dialog is displayed:


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
169 . 254 . 1 . 3
Subnet mask:
255 . 255 . 0 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

3 Enter an IP address that is valid for the 169.254.X.X network, avoiding:

169.254.0.0 and 169.254.1.1

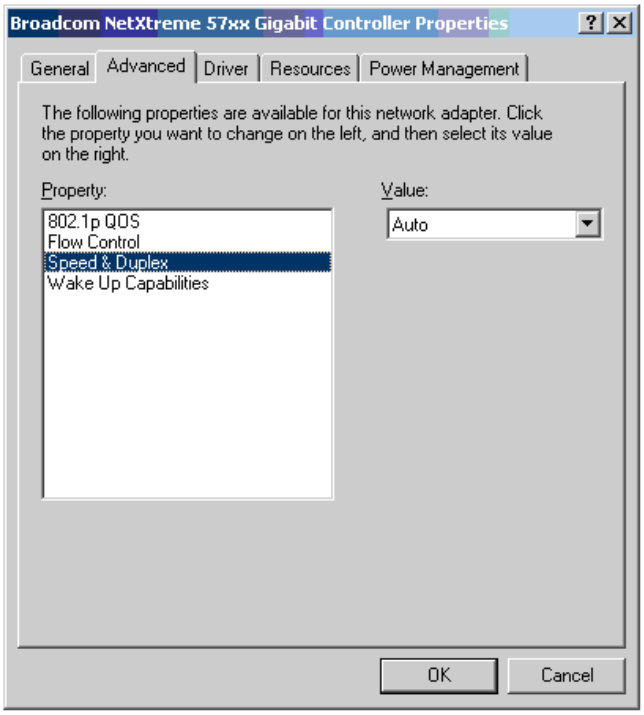
A good example is 169.254.1.3 as shown.

4 Enter a subnet mask of 255.255.0.0.

Leave the default gateway blank.

5 Click on **OK**.

6 If the network adaptor supports advanced properties, then configure Ethernet Speed and Duplex for automatic negotiation. One example, based on a Broadcom™ adaptor, is shown:



Updating the ARP table

All PTP 800 units are supplied by Cambium with the same default IP address. When the management PC is connected to a PTP 800 unit, it creates an association between the default IP address (169.254.1.1) and the MAC address of the PTP 800.

If two or more PTP 800 units are being configured, then remove this association after each unit has been configured. To remove the association between IP address and MAC address in the ARP table of the management PC: open a command prompt window on the PC and enter this command:

```
arp –d 169.254.1.1
```

When this address is next used, the PC will connect it with the MAC address of the unit being configured and update the ARP table with the new association.

Connecting to the PC and powering up

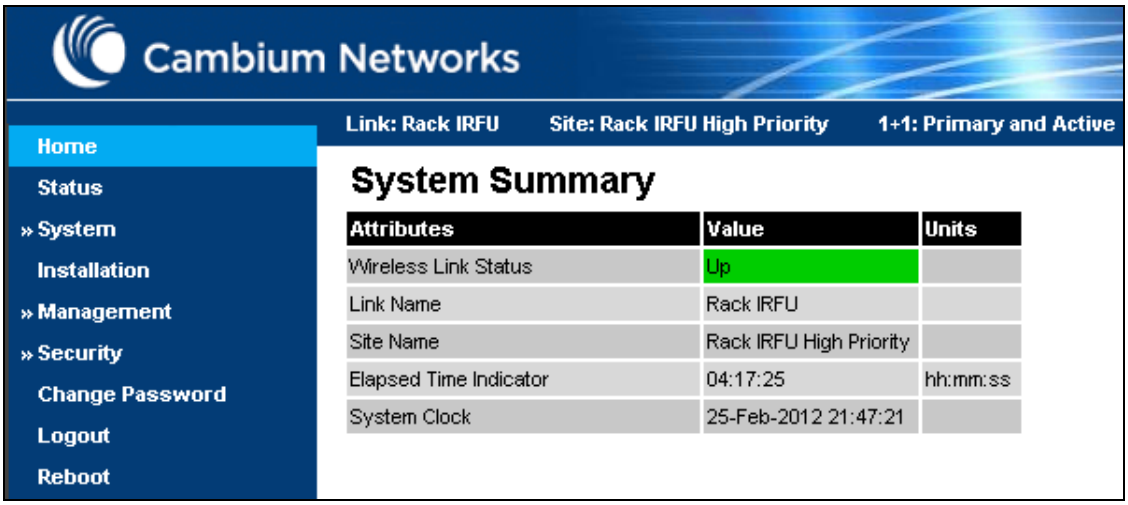
Connect the PC Ethernet port to the Management port of the CMU using a straight-through or crossed Cat5e cable. Switch on the CMU power supply. Wait until the CMU status indicator shows green steady or green slow blink. This normally occurs within 60 seconds from applying power.

Logging into the web interface

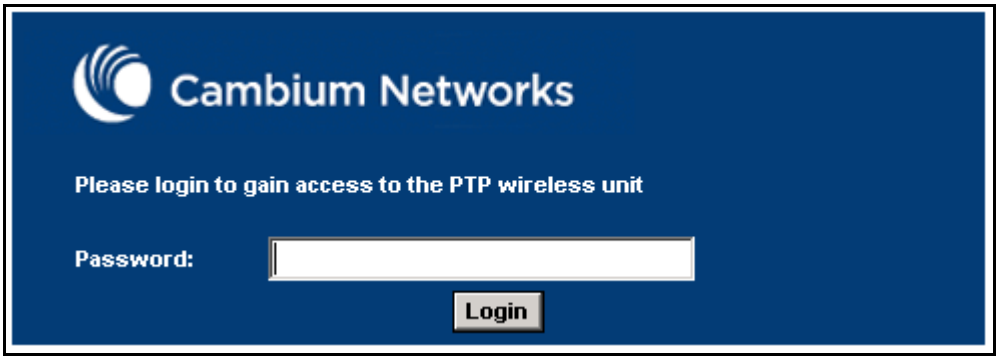
> **NOTE**
> If the management PC is connected to another LAN it may need to be configured to not use proxy servers for this IP address.

To log into the CMU web interface, proceed as follows:

1. Start the web browser from the management PC.
2. Type this IP address of the unit into the address bar: 169.254.1.1
3. Press ENTER. The web interface menu and System Summary page are displayed:



4 Select menu option **System Administration**. The login page is displayed:



5 Leave the Password blank and select **Login**.

Task 2: Configuring IP and Ethernet interfaces

This task consists of the following procedures:

- Managing the units during configuration and alignment on page 6-8
- Configuring the IP interface and management mode on page 6-10
- Reconnecting to the management PC on page 6-19

Managing the units during configuration and alignment

Choose the best way to manage the PTP 800 units during the configuration and alignment process.

Out-of-band management

Where out-of-band management is chosen, the management port is active and a PC can be locally connected. Once the wireless link is operational, the remote PTP 800 unit may also be accessed across the wireless link.

In a 1+1 Hot Standby link with out-of-band management, connect to both PTP 800s in one of the following ways:

- Locally from the Ethernet port of the protection splitter
- From a PC connected to a local switch where routing and connectivity exist for accessing the Ethernet port of the protection splitter.
- Before the protection splitter is installed, locally from the management port.

In-band management

Where in-band management is chosen, the choice of scheme depends on the available data network and the method of network connectivity.

With in-band management, there is a risk that a configuration error could lead to loss of management connectivity. If connectivity is lost, recover the units to a known working saved configuration, as described in Using recovery mode on page 7-71.

In a 1+1 Hot Standby link with in-band management, connect to both PTP 800s in one of the following ways:

- **On the bench, via a local router**: Configure and test the final data port configuration "on the bench". Access for commissioning will be available from a port on a locally connected switch or router. This has the advantage that simultaneous access is possible to both the CMUs being installed.
- **On the bench, via the management network**: As above, but with a connection to a management centre (not across the wireless link being installed) where a co-worker is able to configure and control the PTP 800 units.
- **Using out-of-band**: Install the CMUs using out-of-band management and configure in-band management on site. However, a protection splitter is required and the management setup needs to be reconfigured. Errors could cause loss of the management connection.
- **Using a local PC**: Use in-band management and connect a PC locally to the copper data port. This is possible if VLAN tagging is disabled. Some reconfiguration may be needed, but if the data network is not fully commissioned this could be an alternative. It is recommended that in the final configuration VLAN tagging is enabled.

Configuring the IP interface and management mode

The IP interface allows users to connect to the PTP 800 web interface, either from a locally connected computer or from a management network.

CAUTION

Before setting Management Mode to 'Out-of-Band' or 'In-Band', configure the local and remote CMUs to have different IP addresses, otherwise the management agent will not be able to distinguish the two CMUs.

Similarly for a 1+1 Hot Standby link, configure all four CMUs to have different IP addresses so that the active and inactive units may be distinguished as well as the local and remote CMUs.

NOTE

Forcing Ethernet configuration is a last resort. Select this option only when problems are experienced with auto-negotiation.

To configure the Ethernet link to run at a fixed speed and duplex, leave Ethernet Auto Negotiation set to 'Enabled' and set Auto Neg Advertisement to the required speed.

To configure the IP interface, proceed as follows:

1. Select menu option **System, Configuration, LAN Configuration**. The LAN Configuration page is displayed (Figure 116).
2. Review and update the IP interface attributes (Table 221).
3. If Management Mode has been set to 'Out-of-Band Local' or 'Out-of-Band', review and update the management port attributes (Table 222).
4. Review and update the data port attributes (Table 223).
5. Review and update the bridging attributes (Table 224).
6. Select Submit Updated System Configuration. The **Confirm LAN configuration** page is displayed (Figure 117).
7. Select **Confirm Changes**.

NOTE

If the IP address is updated, then selecting **Submit Updated System Configuration** will change the IP address and communication between the management PC and the CMU will be terminated. To continue configuration, re-connect to the new IP address as described in Reconnecting to the management PC on page 6-19. In case of error see Resetting IP and Ethernet configuration to factory defaults on page 7-75.

NOTE

The SFP Configuration page is only displayed when an SFP module is installed.

Figure 116 LAN Configuration page with VLAN disabled

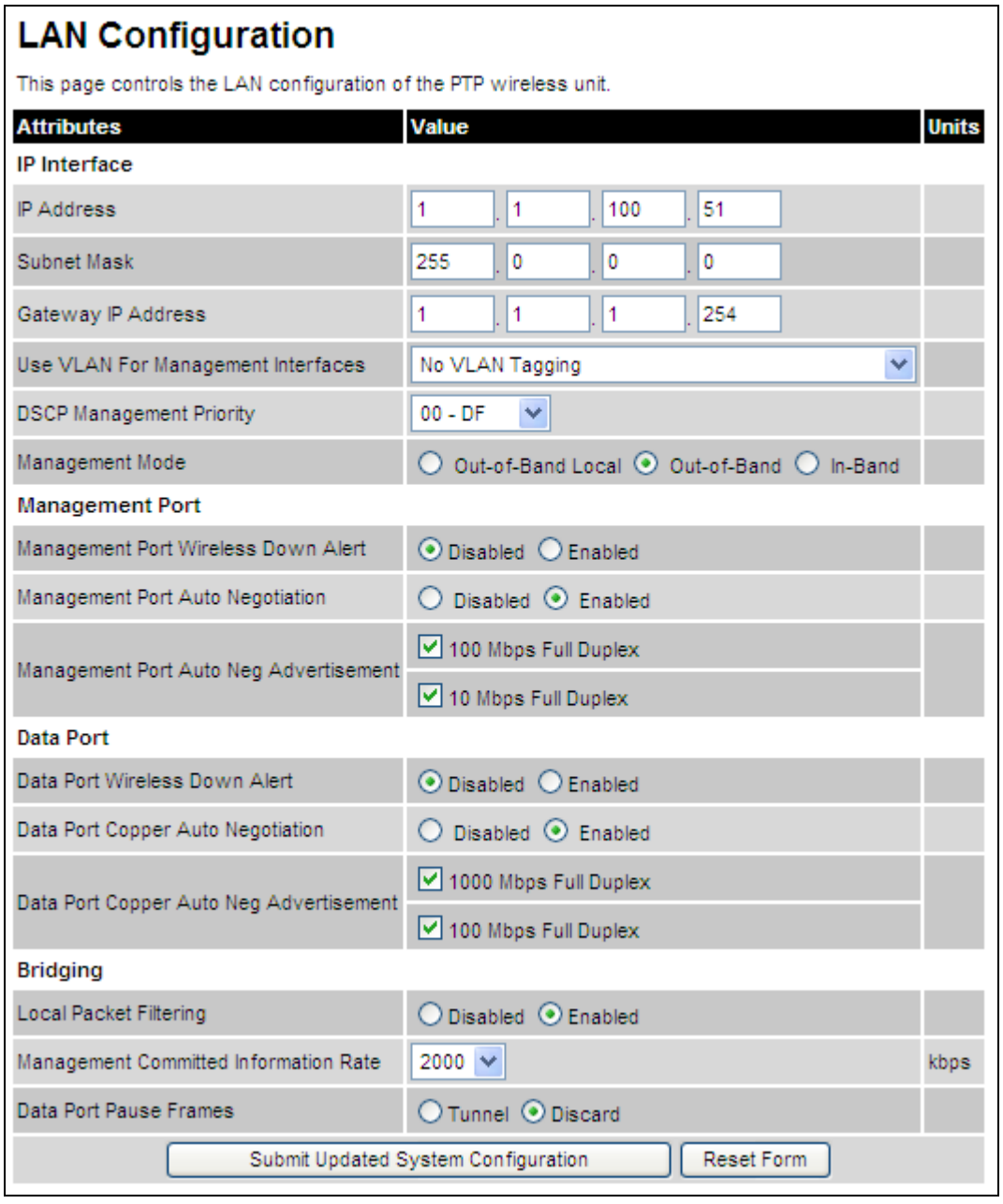


Table 221 IP interface attributes

Attribute	Meaning
IP Address	Internet protocol (IP) address. This address is used by the family of internet protocols to uniquely identify the unit on a network. The default IP address of the management agent is 169.254.1.1.
Subnet Mask	Defines the address range of the connected IP network.
Gateway IP Address	The IP address of a computer on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
Use VLAN For Management Interface	This controls whether or not the management interfaces (WWW/SNMP/SMTP/SNTP) use VLAN tags. Ensure that the configured VLAN is accessible, otherwise it will not be possible to access the unit following the next reboot.
DSCP Management Priority	The Differentiated Services Code Point value. This is inserted in the IP header of all IP datagrams transmitted by the management interfaces.
VLAN Management VID	Only displayed when 'Use VLAN for Management Interfaces' is enabled. Enter the VLAN VID (range 0 to 4094) that will be included in Ethernet frames generated by the management interfaces.
VLAN Management Priority	Only displayed when 'Use VLAN for Management Interfaces' is enabled. Enter the VLAN priority (range 0 to 7) that will be included in Ethernet frames generated by the management interfaces.

Attribute	Meaning
Management Mode	'Out-of-Band Local' means that the web interface can be reached from the management port at the local CMU only. This mode allows the construction of a management network that is isolated from the customer network. This is the default mode. For more information, see Out-of-band local management on page 1-44. 'Out-of-Band' means that the web interface can be reached from the management port at both the local and remote CMUs (assuming that the wireless link is established). For a 1+1 Hot Standby link, configuration access to the remote inactive unit requires connectivity between the management ports. For more information, see Out-of-band management on page 1-44. If 'Out-of-Band' is selected, remember to set the Management Committed Information Rate (Table 224). 'In-Band' means that the web interface can be reached from the data port at both the local and remote CMUs (assuming that the wireless link is established). In this mode, the management port is disabled. For a 1+1 Hot Standby link, connectivity must be provided between the CMU data ports by the customer's network. For more information, see In-band management on page 1-45. For in-band and out-of-band remote management after installation, all four units providing a 1+1 Hot Standby link are accessible from the user interface of each unit.

Table 222 Management port attributes

Attribute	Meaning
Management Port Wireless Down Alert	Only displayed when the Management Mode attribute is set to 'Out-of-Band Local'. If a condition is detected where the link can no longer forward management traffic in one or both directions, for example, a wireless fade or equipment failure, then if this attribute is enabled the management port will be briefly disconnected from the network. This signals to the connected network equipment that this link is no longer available for management traffic. Enabling this feature can be beneficial in complex networks where alternative routes provide continued service in the event of link failure (see Wireless link down alert on page 1-45).
Management Port Auto Negotiation	'Enabled' means that configuration of the out-of-band management Ethernet interface is automatically negotiated. This is the default setting. 'Disabled' means that configuration is forced. Use the same setting for both ends of the link. **⚠ CAUTION** Ensure that this attribute has the same setting in the CMU and in connected network equipment. If they are not consistent, then a duplex mismatch will occur, resulting in greatly reduced data capacity.

Attribute	Meaning
Management Port Auto Neg Advertisement	Select the data rate that the auto-negotiation mechanism will advertise as available on the out-of-band management Ethernet interface. Use the same setting for both ends of the link. **⚠ CAUTION** Ensure that this attribute has the same setting in the CMU and in connected network equipment. If they are not consistent, then a duplex mismatch will occur, resulting in greatly reduced data capacity. **⚠ CAUTION** Only select a data rate that is within the capability of connected network equipment, otherwise loss of service may occur.

Table 223 Data port attributes

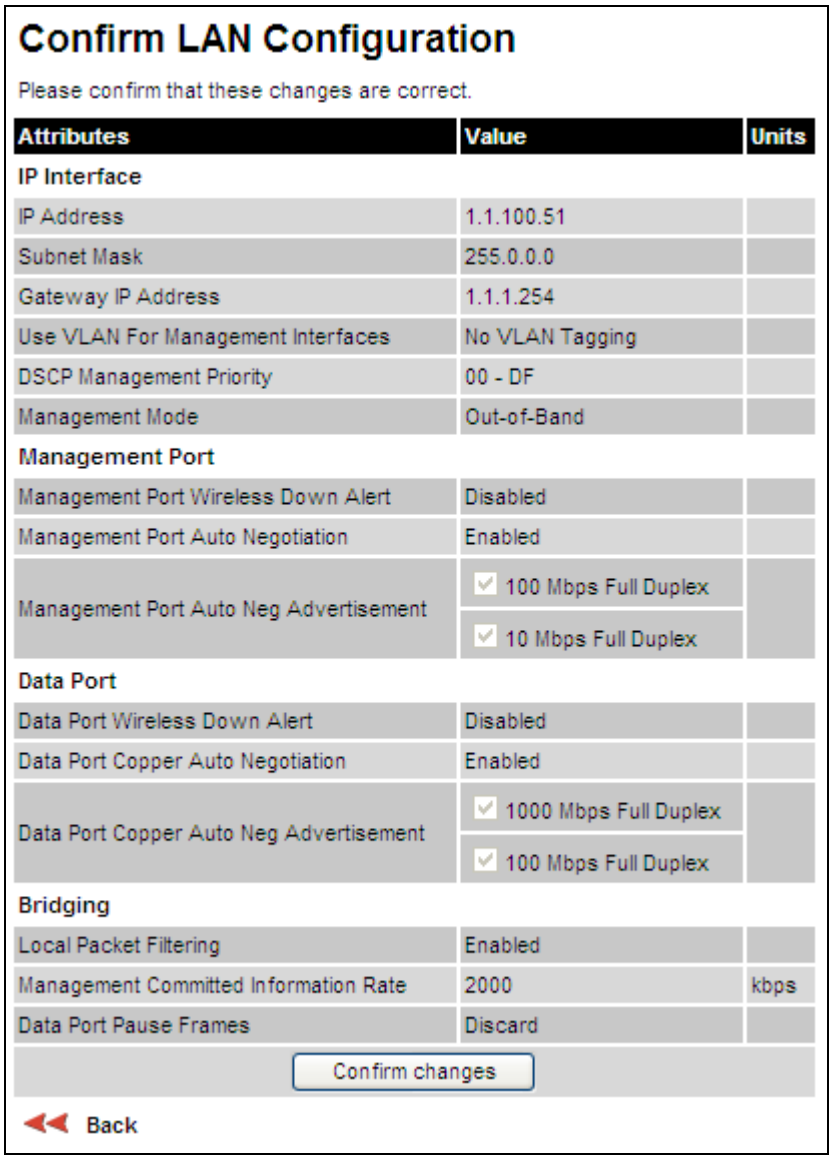
Attribute	Meaning
Data Port Wireless Down Alert	If a condition is detected where the link can no longer forward customer data traffic in one or both directions, for example, a wireless fade or equipment failure, then if this attribute is enabled the data port will be briefly disconnected from the network. This signals to the connected network equipment that this link is no longer available for data traffic. Enabling this feature can be beneficial in complex networks where alternative routes provide continued service in the event of link failure (see Wireless link down alert on page 1-45).
Data Port Ethernet Media Type To Use	Only displayed when an SFP module is installed. 'Auto with Fiber Preference' means that if a supported SFP module is present and is working, and the fiber carrier is present, the Ethernet service connects through fiber and the copper data port is not used. If the fiber link fails or loses the carrier signal, the Ethernet service falls back to the copper LAN connection. 'Force Copper' means that the Ethernet service connects through the copper port only and the Fiber SFP interface is disabled.
Data Port Copper Auto Negotiation	'Enabled' means that configuration is automatically negotiated. This is the default setting. 'Disabled' means that configuration is forced. Use the same setting for both ends of the link. **⚠ CAUTION** Ensure that this attribute has the same setting in the CMU and in connected network equipment. If they are not consistent, then a duplex mismatch will occur, resulting in greatly reduced data capacity.

Attribute	Meaning
Data Port Copper Auto Neg Advertisement	Select the data rate that the auto-negotiation mechanism will advertise as available. Use the same setting for both ends of the link. **⚠ CAUTION** Ensure that this attribute has the same setting in the CMU and in connected network equipment. If they are not consistent, then a duplex mismatch will occur, resulting in greatly reduced data capacity. **⚠ CAUTION** Only select a data rate that is within the capability of connected network equipment, otherwise loss of service may occur.

Table 224 Bridged Ethernet traffic attributes

Attribute	Meaning
Local Packet Filtering	If Local Packet Filtering is enabled, the management agent learns the location of end stations from the source addresses in received management frames. The agent filters transmitted management frames to ensure that the frame is transmitted at the Ethernet (data or management) port, or over the wireless link as appropriate. If the end station address is unknown, then management traffic is transmitted at the Ethernet port and over the wireless link. In out-of-band local management mode, management frames are not transmitted over the wireless link, and so address learning is not active.
Management Committed Information Rate	Only displayed when Management Mode is set to 'Out-of-Band'. Select the minimum data rate (range 200 to 2000 Kbit/s) that the network will guarantee to be available for management traffic.
Data Port Pause Frames	'Tunnel' means that the bridge tunnels Layer 2 PAUSE frames arriving at the Data Port. 'Discard' means that the bridge discards Layer 2 PAUSE frames arriving at the Data Port. Pause frames are identified by the destination MAC Address being equal to 01-80-C2-00-00-01

Figure 117 Confirm LAN Configuration



Confirm LAN Configuration

Please confirm that these changes are correct.

Attributes	Value	Units
IP Interface		
IP Address	1.1.100.51	
Subnet Mask	255.0.0.0	
Gateway IP Address	1.1.1.254	
Use VLAN For Management Interfaces	No VLAN Tagging	
DSCP Management Priority	00 - DF	
Management Mode	Out-of-Band	
Management Port		
Management Port Wireless Down Alert	Disabled	
Management Port Auto Negotiation	Enabled	
Management Port Auto Neg Advertisement	☑ 100 Mbps Full Duplex ☑ 10 Mbps Full Duplex	
Data Port		
Data Port Wireless Down Alert	Disabled	
Data Port Copper Auto Negotiation	Enabled	
Data Port Copper Auto Neg Advertisement	☑ 1000 Mbps Full Duplex ☑ 100 Mbps Full Duplex	
Bridging		
Local Packet Filtering	Enabled	
Management Committed Information Rate	2000	kbps
Data Port Pause Frames	Discard	

Confirm changes

Back

Reconnecting to the management PC

If the IP Address, Subnet Mask and Gateway IP Address of the unit have been updated to meet network requirements, then reconfigure the local management PC to use an IP address that is valid for the network. Refer to Configuring the management PC on page 6-3.

When the IP address of the unit has been reconfigured, log in using the new IP address. Refer to Logging into the web interface on page 6-6.

NOTE

Access to the CMU can be recovered using Recovery mode as described in Resetting IP and Ethernet configuration to factory defaults on page 7-75.

Task 3: Installing license keys

This task consists of the following procedures:

- Checking licensed capabilities on page 6-21
- Generating a new license key on page 6-23
- Entering a new license key on page 6-23
- Starting the full capacity trial on page 6-24

Some PTP 800 products are supplied with two license keys: one installed at the factory and one alternative key.

NOTE

A license key is not required in order to enable the 1+1 protection capability. Each of the PTP 800s in the protection scheme is individually licensed and configured with its own license key for the capacity of the link.

Checking licensed capabilities

To check that the installed license key provides the required capabilities, select menu option **System, License Key**. The Software License Key page is displayed (Figure 118). Check the attributes in the Capability summary section (Table 225).

CAUTION

Check that these attributes (other than MAC Address) are the same at both link ends, otherwise the link will not operate correctly.

If any of the required capabilities are not provided, then perform Generating a new license key on page 6-23.

Figure 118 Software License Key page

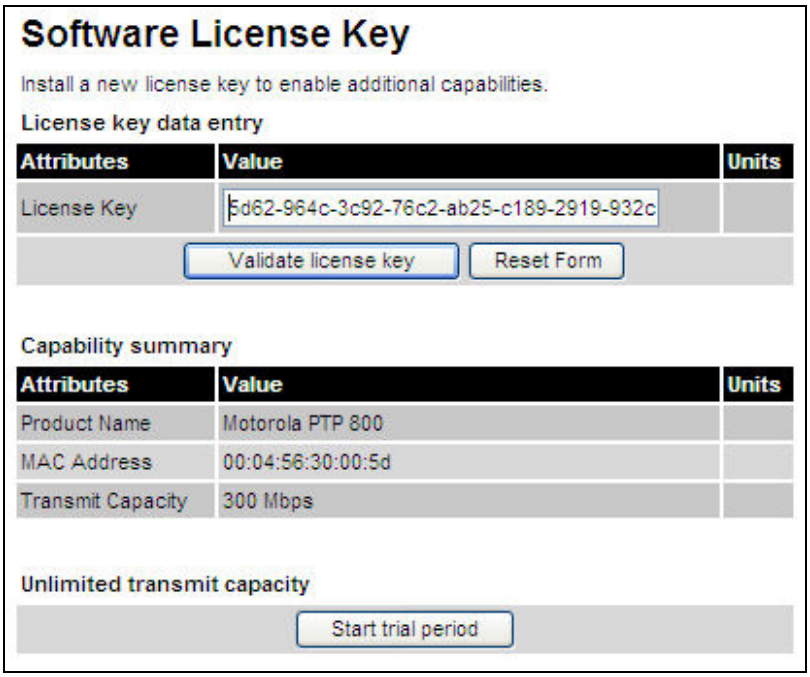


Table 225 Capability summary attributes

Attribute	Meaning
Product Name	The name of the PTP 800 product variant.
MAC Address	The MAC address of the PTP 800.
FIPS Security Level	The maximum configurable security level. **NOTE** If FIPS 140-2 capability is required, ensure that the FIPS Security Level is set to 'FIPS'.
Encryption Algorithm	The encryption algorithms available for use at the wireless interface of the CMU. This attribute is only displayed if the current license key permits encryption. This attribute must be the same at both link ends. To determine upgrade requirements, see AES license on page 1-60.

Attribute	Meaning
Transmit Capacity	Maximum permitted data rate for Ethernet frames. The actual data rate depends upon the prevailing wireless conditions. The application software does permit a link to be established between units with different Transmit Capacity values. **NOTE** A full capacity trial period may be available on this unit. For more information, see Starting the full capacity trial on page 6-24.

Generating a new license key

To generate a new license key to activate new licensed capabilities (for example activate AES encryption or increase transmit capacity), proceed as follows:

1. Purchase the required new capabilities from the Cambium authorized Point-To-Point dealer who supplied the link. The dealer will supply one or more access keys.
2. Go to the PTP web support page (see Contacting Cambium Networks on page 2).
3. Select **Key Generator**. The PTP License Key Generator form should be displayed.
4. Enter the required details, including the access keys supplied by the dealer.
5. Submit the web form. The PTP License Key Generator will respond with the new license key.

Entering a new license key

To upgrade the unit to a new license key, select menu option **System, License Key**. The Software License Key page is displayed (Figure 118). Enter the new License Key and select **Validate license key**. If the license key is valid, a confirmation message is displayed. Select **OK** to confirm. The new license key is installed in the unit.

Starting the full capacity trial

The full capacity trial period allows a unit that has a limited data throughput capacity (up to 300 Mbps) to operate with full transmit capacity (unlimited) during a trial period of duration 60 days, reverting to the limited capacity when the trial period expires.

The full capacity trial period is available on:

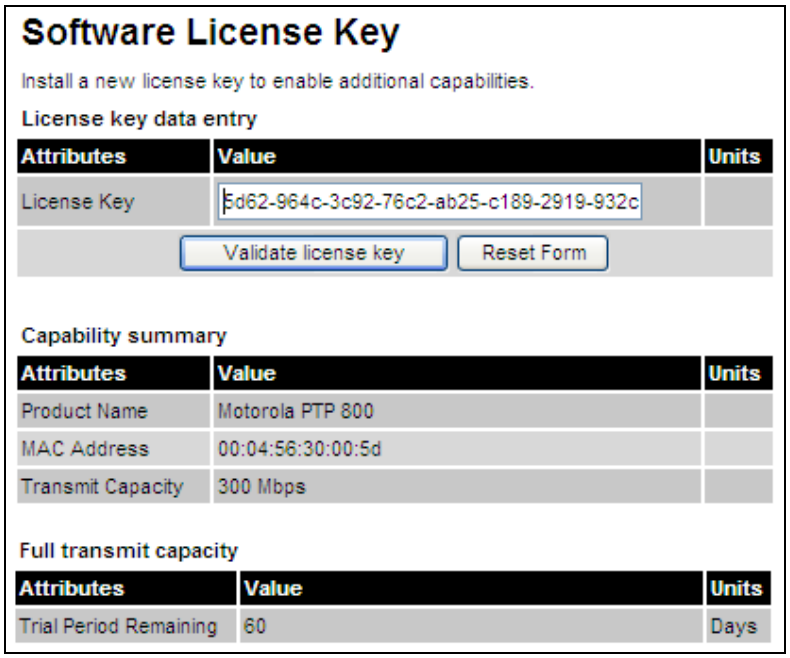
- Newly purchased PTP 800 units.
- Existing PTP 800 units that are upgraded to System Release 800-04-00 or a later release.

If a full capacity trial is pending on this unit, the Software License Key page contains a trial period start control (Figure 118). To start the trial period, select **Start trial period**; when the confirmation message is displayed, select **OK**.

NOTE
To allow full transmit capacity, start the trial period at both link ends.

When the trial has started, the Software License Key page displays the Trial Period Remaining attribute (Figure 119). This shows the time remaining (in days, hours or minutes) before the full capacity trial period expires.

Figure 119 Software License Key page with full capacity trial in progress



When the trial has ended, the Software License Key page displays a message.

Task 4: Upgrading software version

This task consists of the following procedures:

- Checking the installed software version on page 6-25
- Upgrading to a new software version on page 6-26

CAUTION

Ensure that the correct units are upgraded, as units cannot easily be downgraded afterwards.

If the link is operational, ensure that the remote end of the link is upgraded first using the wireless connection, and then the local end can be upgraded. Otherwise, the remote end may not be accessible.

NOTE

Load the standard (non-FIPS) software image for 800-04-00 or later before loading a FIPS software image.

Checking the installed software version

To check the installed software version, select menu option **Status**. The System Status page is displayed. Software Version is in the CMU section (Figure 120).

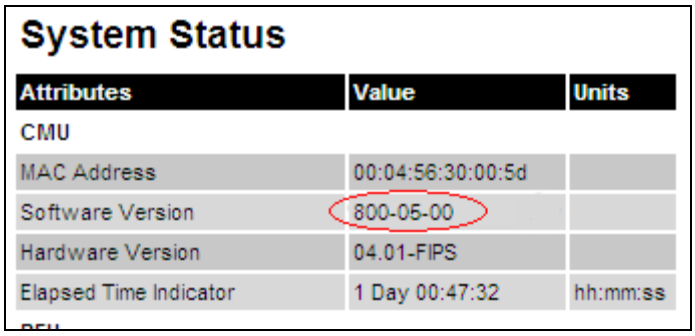
If FIPS capability is required, check that the installed software is FIPS validated, as indicated by a `-FIPS` prefix to the Software Version, for example:

```
FIPS-PTP800-04-10
```

Go to the support web page (see Contacting Cambium Networks on page 2) and find Point-to-Point software updates. Check that the latest software version (for example 800-04-10) is the same as the installed Software Version.

If the software needs to be upgraded to the latest version, perform Upgrading to a new software version on page 6-26.

Figure 120 Software Version in System Status page



Upgrading to a new software version

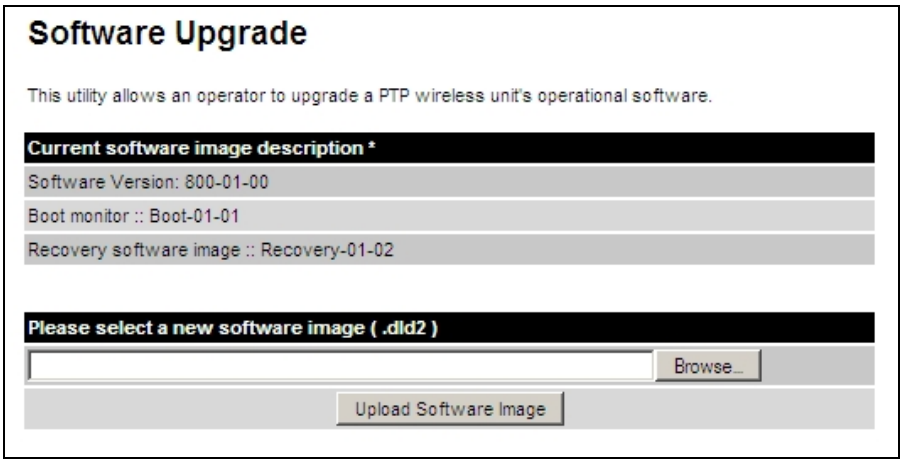
Perform this task to upgrade the units to a new version of PTP 800 operational software.

CMU software version must be the same at both ends of the link. Limited operation may sometimes be possible with dissimilar software version, but such operation is not supported by Cambium.

Upgrade the remote end of a link before upgrading the local end, and for a 1+1 Hot Standby link upgrade the inactive units and force a protection switch to them before upgrading the active units. This approach maximizes system availability.

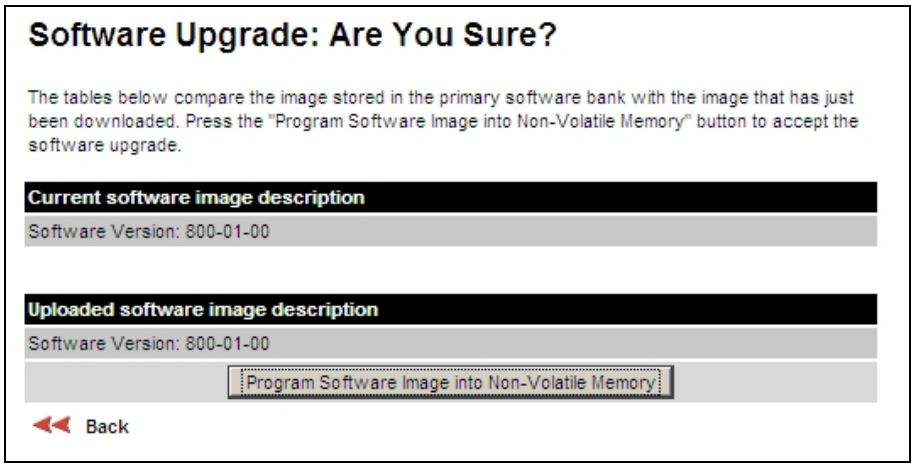
To upgrade the software, proceed as follows:

1. Save the pre-upgrade system configuration as described in Saving the system configuration on page 6-119.
2. Go to the support web page (see Contacting Cambium Networks on page 2) and find Point-to-Point software updates. Download and save the required software image (for example PTP 800-nn-mm.dld2 or PTP 800-nn-mm-FIPS.dld2).
3. Select menu option **System, Software Upgrade**. The Software Upgrade page is displayed:


Software Upgrade
This utility allows an operator to upgrade a PTP wireless unit's operational software.
Current software image description *
Software Version: 800-01-00
Boot monitor :: Boot-01-01
Recovery software image :: Recovery-01-02
Please select a new software image (.dld2)
Browse...
Upload Software Image

4 Select **Browse**. Navigate to the folder containing the downloaded software image and select **Open**.

5 Select **Upload Software Image**. The Software Upgrade Confirmation page is displayed:


Software Upgrade: Are You Sure?
The tables below compare the image stored in the primary software bank with the image that has just been downloaded. Press the "Program Software Image into Non-Volatile Memory" button to accept the software upgrade.
Current software image description
Software Version: 800-01-00
Uploaded software image description
Software Version: 800-01-00
Program Software Image into Non-Volatile Memory
Back

If the upgrade is taking the CMU into or out of FIPS mode, an additional warning is displayed stating that the upgrade will cause automatic erasure of the critical security parameters (CSPs).

6 Select **Program Software Image into Non-Volatile Memor**y. The Progress Tracker page is displayed. On completion, the Software Upgrade Complete page is displayed:


Software Upgrade Complete
The software upgrade was completed Successfully. To complete the upgrade a system reboot is required. Please use the 'Reboot Wireless Unit' button below to reboot the unit.
Current software image description
Software Version: 800-01-00
Reboot Wireless Unit
Back

7 Select **Reboot Wireless Unit**. Select **OK** to confirm. The unit reboots with the new software installed.

8 Save the post-upgrade system configuration as described in Saving the system configuration on page 6-119.

Task 5: Configuring security

Perform this task to configure the PTP 800 in accordance with the network security policy. Choose from the following procedures:

- Configuring AES encryption on page 6-29: to configure AES link encryption without HTTPS/TLS.
- Configuring AES encryption in an operational link on page 6-31: to enable AES encryption over an operational link.
- Configuring HTTPS/TLS on page 6-32: to configure the unit to operate in HTTPS/TLS mode.
- Configuring local user accounts on page 6-42: to set user account options, password complexity and identity-based users.
- Changing own user password on page 6-48: for any user to change their own password.
- Protecting access to the summary and status pages on page 6-49: to apply password access to the System Summary and System Status pages.
- Configuring RADIUS authentication on page 6-50: to configure RADIUS server authentication of PTP 800 users.

NOTE

If FIPS 140-2 secure mode is required, please refer to Configuring for FIPS 140-2 applications on page 6-121 instead of Configuring HTTPS/TLS on page 6-32.

CAUTION

Ensure that the network requirements are configured before connecting the PTP 800 to the network. Otherwise, security may be compromised.

Configuring AES encryption

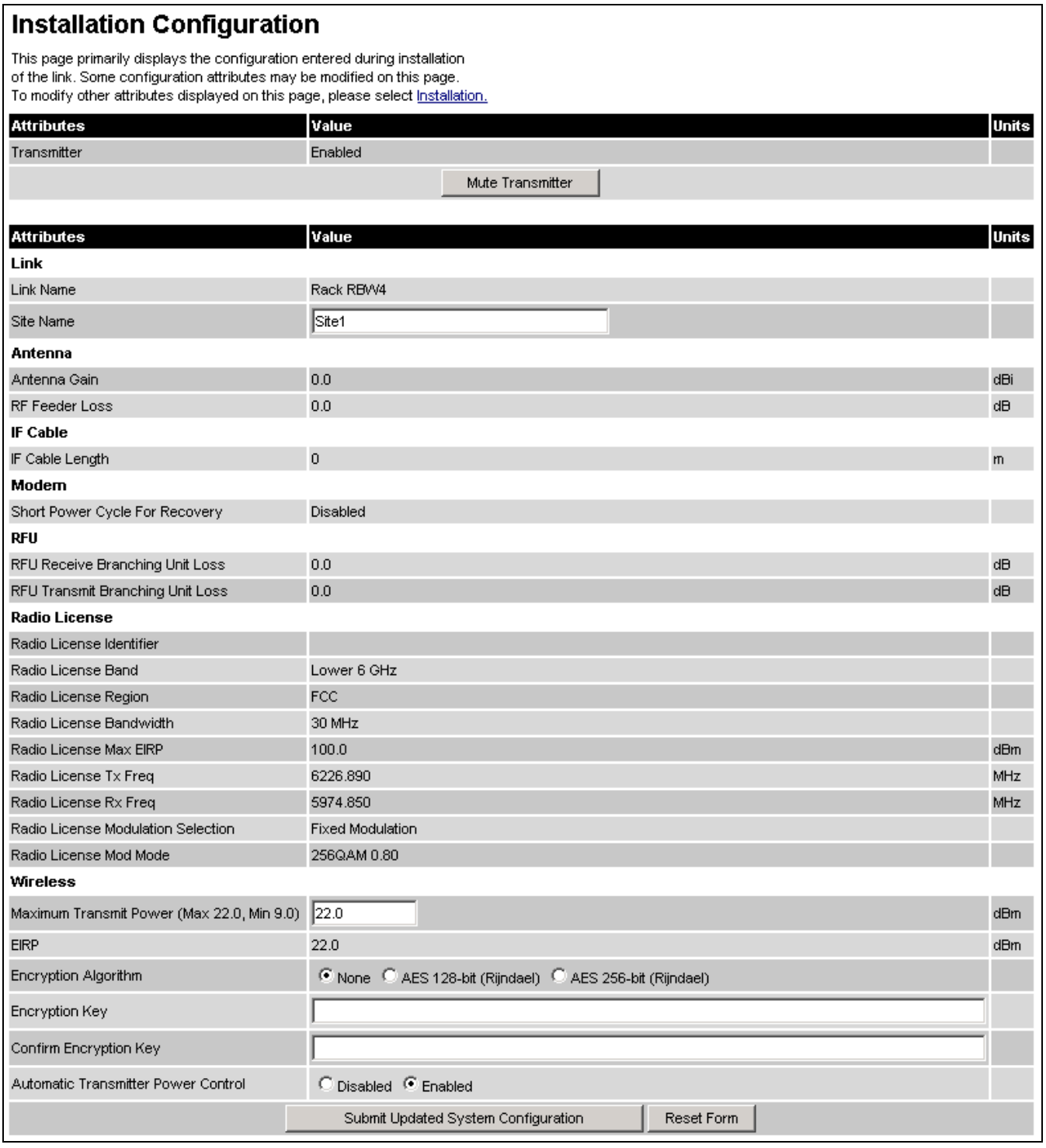
To configure AES link encryption (before the link is operational), proceed as follows:

1. Check the capability summary in the Software License Key page to ensure that the current license key supports AES. If necessary, obtain an access key and generate a new license key, as described in Task 3: Installing license keys on page 6-21.
2. Select menu option **System, Configuration**. The Installation Configuration page is displayed (Figure 121).
3. Select the Encryption Algorithm, either ‘AES 128-bit’ or ‘AES 256-bit’. The same algorithm must be used at both ends of the link.
4. Enter and confirm the encryption key. The key consists of 32 or 64 case-insensitive hexadecimal characters. The same key must be used at both ends of the link.
5. Select **Submit Updated System Configuration**. The reboot confirmation dialog is displayed:


The Configuration Changes Require a System Reboot
The configuration changes you requested can only be activated via a system reboot. Would you like to reboot the wireless unit now?
Reboot Wireless Unit
Back

6. Select **Reboot Wireless Unit** and then **OK** to confirm.

Figure 121 Installation Configuration page



Installation Configuration

This page primarily displays the configuration entered during installation of the link. Some configuration attributes may be modified on this page. To modify other attributes displayed on this page, please select Installation.

Attributes	Value	Units
Transmitter	Enabled	
	Mute Transmitter	

Attributes	Value	Units
Link		
Link Name	Rack RBW4	
Site Name	Site1	
Antenna		
Antenna Gain	0.0	dBi
RF Feeder Loss	0.0	dB
IF Cable		
IF Cable Length	0	m
Modem		
Short Power Cycle For Recovery	Disabled	
RFU		
RFU Receive Branching Unit Loss	0.0	dB
RFU Transmit Branching Unit Loss	0.0	dB
Radio License		
Radio License Identifier		
Radio License Band	Lower 6 GHz	
Radio License Region	FCC	
Radio License Bandwidth	30 MHz	
Radio License Max EIRP	100.0	dBm
Radio License Tx Freq	6226.890	MHz
Radio License Rx Freq	5974.850	MHz
Radio License Modulation Selection	Fixed Modulation	
Radio License Mod Mode	256QAM 0.80	
Wireless		
Maximum Transmit Power (Max 22.0, Min 9.0)	22.0	dBm
EIRP	22.0	dBm
Encryption Algorithm	None / AES 128-bit (Rijndael) / AES 256-bit (Rijndael)	
Encryption Key		
Confirm Encryption Key		
Automatic Transmitter Power Control	Disabled / Enabled	
	Submit Updated System Configuration / Reset Form	

Configuring AES encryption in an operational link

⚠ CAUTION

Configuring link encryption over an operational link will necessitate a service outage. Therefore, the configuration process should be scheduled during a period of low link utilization.

To enable AES encryption over an operational link, proceed as follows:

1. Open two browsers.
2. Log into the web interfaces at each end of the link.
3. Perform Configuring AES encryption on page 6-29 at each unit.
4. Reboot both ends of the link.
5. The software is designed to allow five seconds so that a user can command both ends of the link to reboot before the wireless link drops.

To enable AES encryption over an operational 1+1 Hot Standby link:

- Configure licence keys on all CMUs, if required to permit use of encryption. See Task 3: Installing license keys on page 6-21.
- Follow the procedure Changing AES encryption keys on page 7-53.

Configuring HTTPS/TLS

Perform this procedure if the unit is required to operate in HTTPS/TLS mode. For more information, refer to Planning for HTTPS/TLS operation on page 2-23.

> **NOTE**
> If FIPS 140-2 secure mode is required, refer to Configuring for FIPS 140-2 applications on page 6-121 instead of this procedure.

To configure HTTPS/TLS, proceed as follows:

1. Ensure that the following cryptographic material has been generated:

   Key Of Keys

   TLS Private Key and Public Certificates (for the correct IP address)

   User Defined Security Banner

   Entropy Input

   Wireless Link Encryption Key for AES

2. Identify the Port numbers for HTTPS, HTTP and Telnet.
3. Ensure that the web browsers used are enabled for HTTPS/TLS operation.
4. Select menu option **Management, Web, Local User Accounts** and check that:

   EITHER: Identity Based User Accounts are ‘Disabled’,

   OR: Identity Based User Accounts are ‘Enabled’. and the current user's role is Security Officer.

5. Perform Task 3: Installing license keys on page 6-21 and ensure that the installed license key meets all requirements including HTTPS/TLS compatibility:

   Check that Encryption Algorithm is ‘AES….’.

   If necessary, generate and enter a new license key with the above settings.

6. To activate HTTPS/TLS mode, perform Using the Security Wizard on page 6-33.

Using the Security Wizard

If the PTP 800 is to operate in secure mode (HTTPS/TLS with or without FIPS 140-2), use the Security Wizard to review and configure HTTPS/TLS security related parameters.

The Security Wizard is only available when both of the following conditions are true:

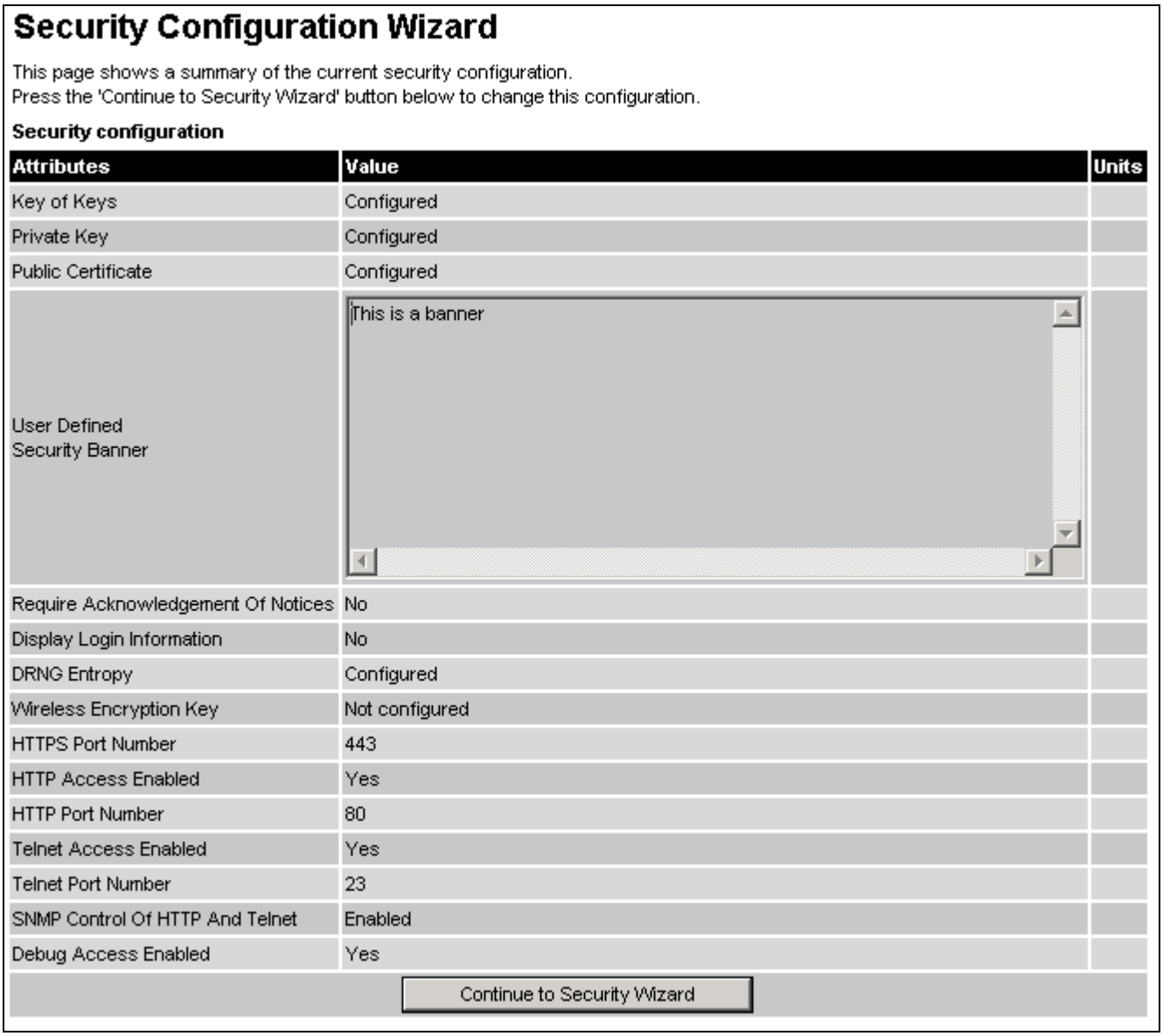
- The wireless unit has a license key with either 128-bit or 256-bit AES link encryption enabled,
- AND:
  - EITHER: identity-based user accounts are disabled,
  - OR: identity-based user accounts are enabled and the user's role is Security Officer.

If these conditions are not both true, the Current Security Summary page prevents execution of the wizard.

Starting Security Wizard

To review HTTPS/TLS security related parameters, select menu option **Security**. The Security Configuration Wizard page is displayed (Figure 122). Review the summary: if any updates are required, select **Continue to Security Wizard**.

Figure 122 Security Configuration Wizard page



Security Configuration Wizard

This page shows a summary of the current security configuration.
Press the 'Continue to Security Wizard' button below to change this configuration.

Security configuration

Attributes	Value	Units
Key of Keys	Configured	
Private Key	Configured	
Public Certificate	Configured	
User Defined Security Banner	This is a banner	
Require Acknowledgement Of Notices	No	
Display Login Information	No	
DRNG Entropy	Configured	
Wireless Encryption Key	Not configured	
HTTPS Port Number	443	
HTTP Access Enabled	Yes	
HTTP Port Number	80	
Telnet Access Enabled	Yes	
Telnet Port Number	23	
SNMP Control Of HTTP And Telnet	Enabled	
Debug Access Enabled	Yes	

Continue to Security Wizard

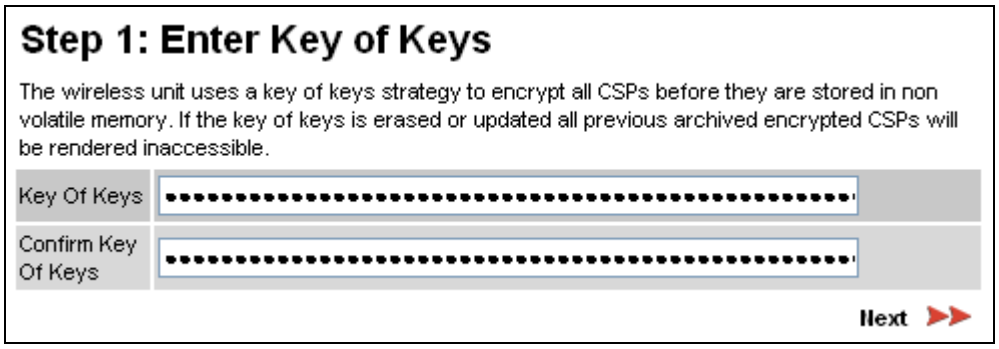
Step 1: Enter key of keys

⚠ CAUTION

Erasing or changing the keys of keys erases all critical security parameters (CSPs).

The Step 1: Enter Key of Keys page is displayed (Figure 123). Enter the generated key of keys in both the Key Of Keys and Confirm Key Of Keys fields. Select **Next**.

Figure 123 Step 1: Enter Key of Keys page


Step 1: Enter Key of Keys
The wireless unit uses a key of keys strategy to encrypt all CSPs before they are stored in non volatile memory. If the key of keys is erased or updated all previous archived encrypted CSPs will be rendered inaccessible.
Key Of Keys
Confirm Key Of Keys
Next

Step 2: TLS private key and public certificate

⚠ CAUTION

If the certificates expire, the unit will be unreachable. If this occurs, put the unit into recovery mode and erase all configuration. For more information, refer to Using recovery mode on page 7-71.

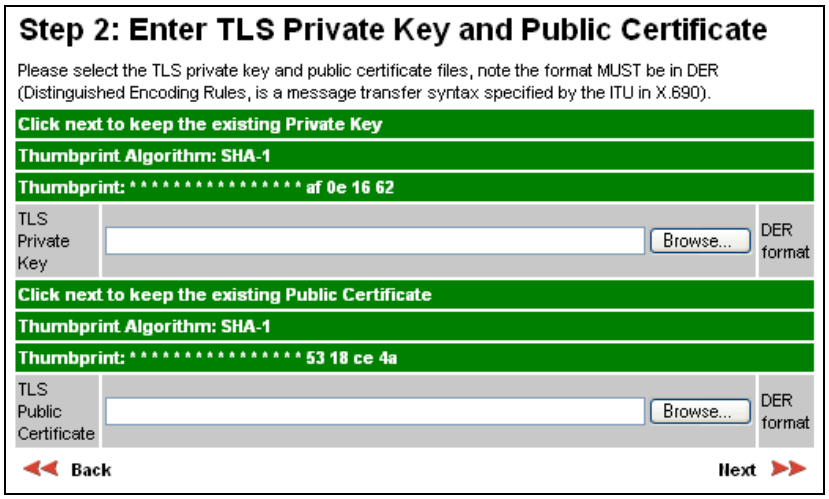
The Step 2: TLS Private Key and Public Certificate page is displayed (Figure 124).

If a valid TLS private key exists, then an SHA-1 thumbprint of the key is displayed. If this key is correct, then take no action. Otherwise, select **Browse** and select the generated private key file (.der).

If a valid TLS public certificate exists, then an SHA-1 thumbprint of the certificate is displayed. If this certificate is correct, then take no action. Otherwise, select **Browse** and select the generated certificate file (.der).

Select **Next**.

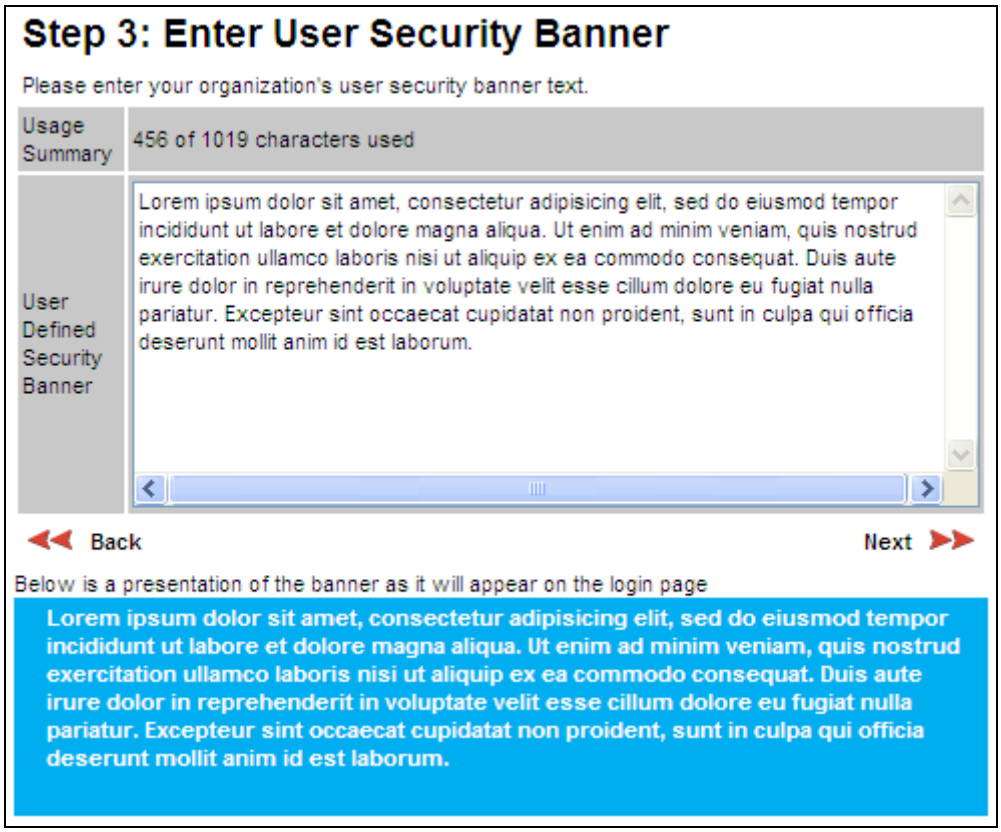
Figure 124 Step 2: TLS Private Key and Public Certificate page


Step 2: Enter TLS Private Key and Public Certificate
Please select the TLS private key and public certificate files, note the format MUST be in DER (Distinguished Encoding Rules, is a message transfer syntax specified by the ITU in X.690).
Click next to keep the existing Private Key
Thumbprint Algorithm: SHA-1
Thumbprint: * * * * * * * * * * * * * * * * af 0e 16 62
TLS Private Key
Browse...
DER format
Click next to keep the existing Public Certificate
Thumbprint Algorithm: SHA-1
Thumbprint: * * * * * * * * * * * * * * * * 53 18 ce 4a
TLS Public Certificate
Browse...
DER format
Back
Next

Step 3: User security banner

The Step 3: User Security Banner page is displayed (Figure 125). Update the User Defined Security Banner field. This banner will be displayed every time a user attempts to login to the wireless unit. Select **Next**

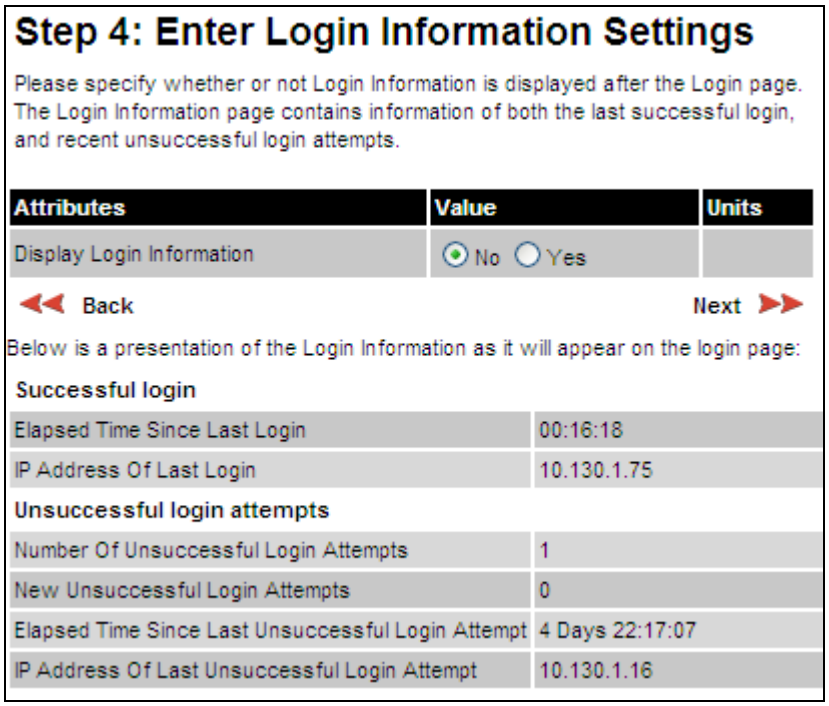
Figure 125 Step 3: User Security Banner page


Step 3: Enter User Security Banner
Please enter your organization's user security banner text.
Usage Summary
456 of 1019 characters used
User Defined Security Banner
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
Back
Next
Below is a presentation of the banner as it will appear on the login page
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Step 4: Login information settings

The Step 4: Login Information Settings page is displayed (Figure 126). Set Display Login Information to 'No' or 'Yes'. Select **Next**.

Figure 126 Step 4: Login Information Settings page

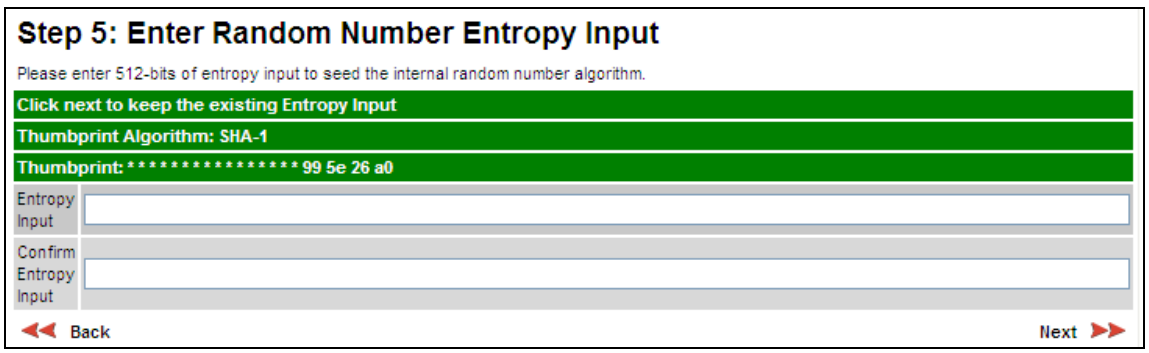

Step 4: Enter Login Information Settings
Please specify whether or not Login Information is displayed after the Login page. The Login Information page contains information of both the last successful login, and recent unsuccessful login attempts.
Attributes
Value
Units
Display Login Information
No
Yes
Back
Next
Below is a presentation of the Login Information as it will appear on the login page:
Successful login
Elapsed Time Since Last Login
00:16:18
IP Address Of Last Login
10.130.1.75
Unsuccessful login attempts
Number Of Unsuccessful Login Attempts
1
New Unsuccessful Login Attempts
0
Elapsed Time Since Last Unsuccessful Login Attempt
4 Days 22:17:07
IP Address Of Last Unsuccessful Login Attempt
10.130.1.16

Step 5: Random number entropy input

The Step 5: Random Number Entropy Input page is displayed (Figure 127). The entropy input is used to seed the TLS random number generator.

If valid entropy input exists, then an SHA-1 thumbprint of the input is displayed. If this input is correct, then take no action. Otherwise, enter the generated input in the Entropy Input and Confirm Entropy Input fields. Select **Next**.

Figure 127 Step 5: Random Number Entropy Input page

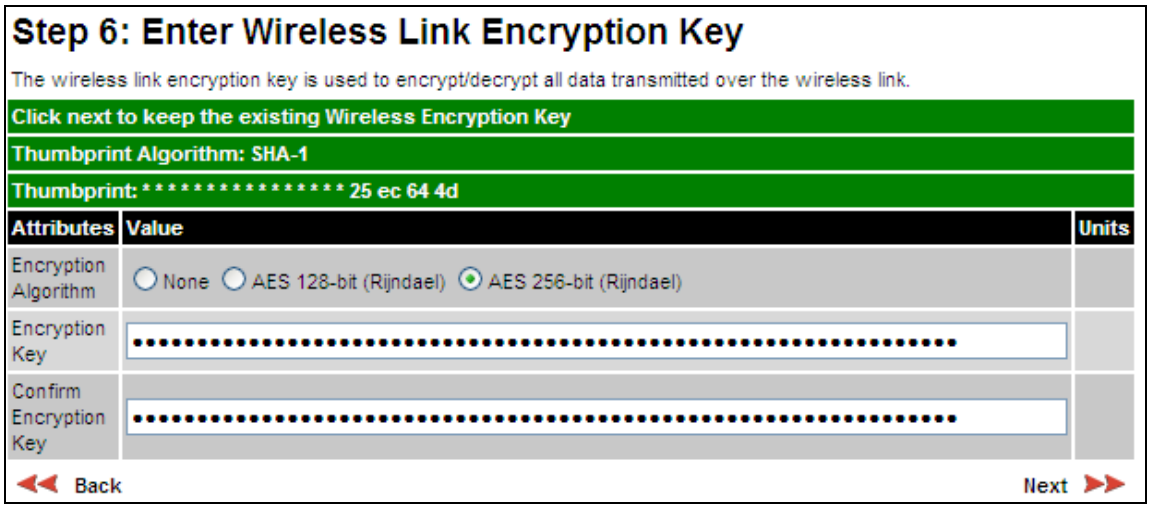

Step 5: Enter Random Number Entropy Input
Please enter 512-bits of entropy input to seed the internal random number algorithm.
Click next to keep the existing Entropy Input
Thumbprint Algorithm: SHA-1
Thumbprint: ********** 99 5e 26 a0
Entropy Input
Confirm Entropy Input
Back
Next

Step 6: Enter the wireless link encryption key

The Step 6: Enter The Wireless Link Encryption Key page is displayed (Figure 128). The wireless link encryption key is used to encrypt all traffic over the PTP 800 wireless link.

Select the applicable value in the Encryption Algorithm field. If a valid encryption key exists, then an SHA-1 thumbprint of the key is displayed. If this key is correct, then take no action. Otherwise, enter the generated key in the Wireless Link Encryption Key and Confirm Wireless Link Encryption Key fields. Select **Next**.

Figure 128 Step 6: Enter Wireless Link Encryption Key page



Step 7: HTTP and Telnet settings

The Step 7: HTTP and Telnet Settings page is displayed (Figure 129). The PTP 800 can be remotely managed in four ways: HTTPS, HTTP, Telnet or SNMP. Review and update the HTTP and Telnet attributes (Table 226). Select **Next**.

Figure 129 Step 7: HTTP and Telnet Settings page

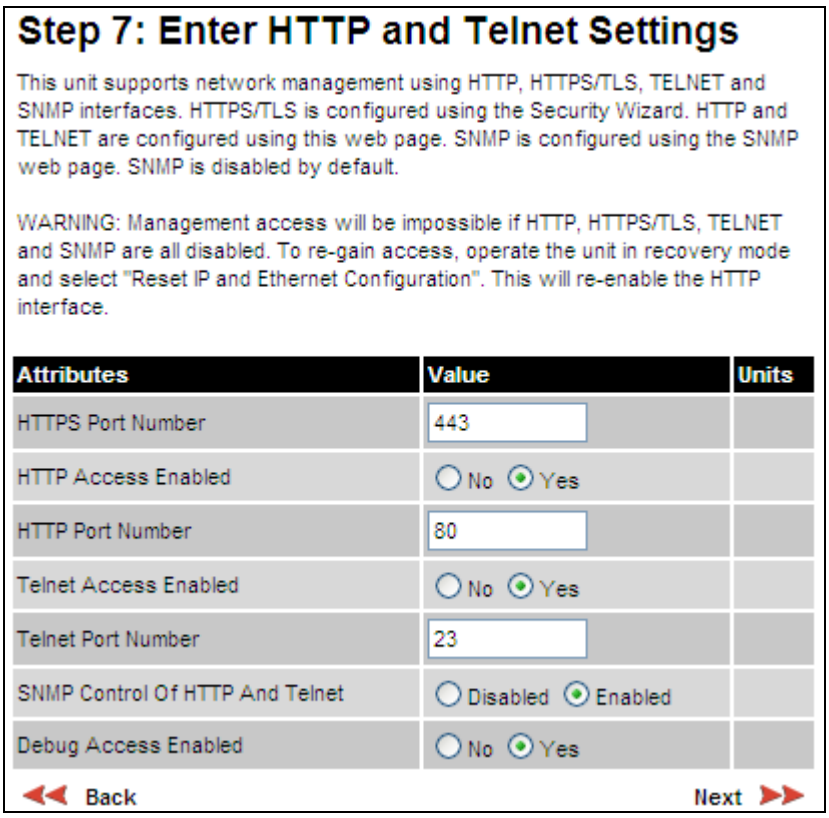

Step 7: Enter HTTP and Telnet Settings
This unit supports network management using HTTP, HTTPS/TLS, TELNET and SNMP interfaces. HTTPS/TLS is configured using the Security Wizard. HTTP and TELNET are configured using this web page. SNMP is configured using the SNMP web page. SNMP is disabled by default.
WARNING: Management access will be impossible if HTTP, HTTPS/TLS, TELNET and SNMP are all disabled. To re-gain access, operate the unit in recovery mode and select "Reset IP and Ethernet Configuration". This will re-enable the HTTP interface.
Attributes
Value
Units
HTTPS Port Number
443
HTTP Access Enabled
No
Yes
HTTP Port Number
80
Telnet Access Enabled
No
Yes
Telnet Port Number
23
SNMP Control Of HTTP And Telnet
Disabled
Enabled
Debug Access Enabled
No
Yes
Back
Next

Table 226 HTTP and Telnet attributes

Attribute	Meaning
HTTPS Port Number	The port number for HTTPS access. A value of zero means the wireless unit uses the default port. **NOTE** HTTPS access is controlled by license key.
HTTP Access Enabled	'No' means that the unit will not respond to any requests on the HTTP port. 'Yes' means that the unit will respond to requests on the HTTP port. Remote management via HTTPS is not affected by this setting.
HTTP Port Number	The port number for HTTP access. A value of zero means the wireless unit uses the default port.
Telnet Access Enabled	'No' means that the unit will not respond to any requests on the Telnet port. 'Yes' means that the unit will respond to requests on the Telnet port.
Telnet Port Number	The port number for Telnet access. A value of zero means the wireless unit uses the default port.
SNMP Control of HTTP And Telnet	'Disabled' means that neither HTTP nor Telnet can be controlled remotely via SNMP. 'Enabled' means that both HTTP and Telnet can be controlled remotely via SNMP.
Debug Access Enabled	'Yes' means that Cambium Technical Support is allowed to access the system to investigate faults.

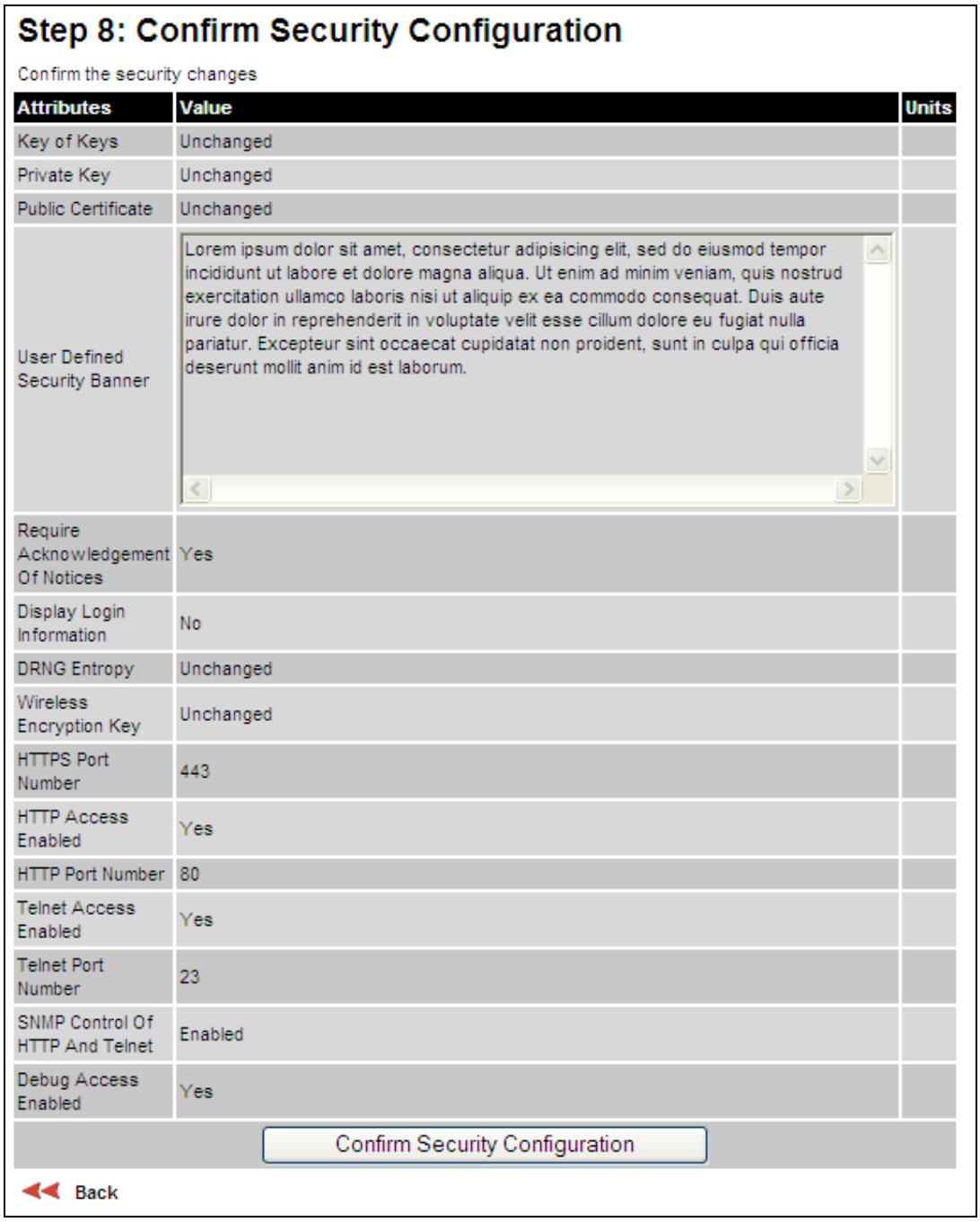
NOTE

If HTTP, Telnet and SNMP are all disabled (as required for FIPS 140-2 mode), the secure web server becomes the only management tool for the CMU web interface. To reenter the web interface after Step 7 of the Security Wizard, use the URL **https://aa.bb.cc.dd** (where aa.bb.cc.dd is the IP address of the unit).

Step 8: Commit security configuration

Review all changes that have been made in the Security Wizard (Figure 130). To ensure that the changes take effect, select **Commit Security Configuration**. The unit reboots and the changes take effect.

Figure 130 Step 8: Commit Security Configuration page



> **NOTE**
> If the Key of keys is entered or modified in the Security Wizard, user accounts are reset when **Commit Security Configuration** is selected. It is then necessary to reconfigure them.

Configuring local user accounts

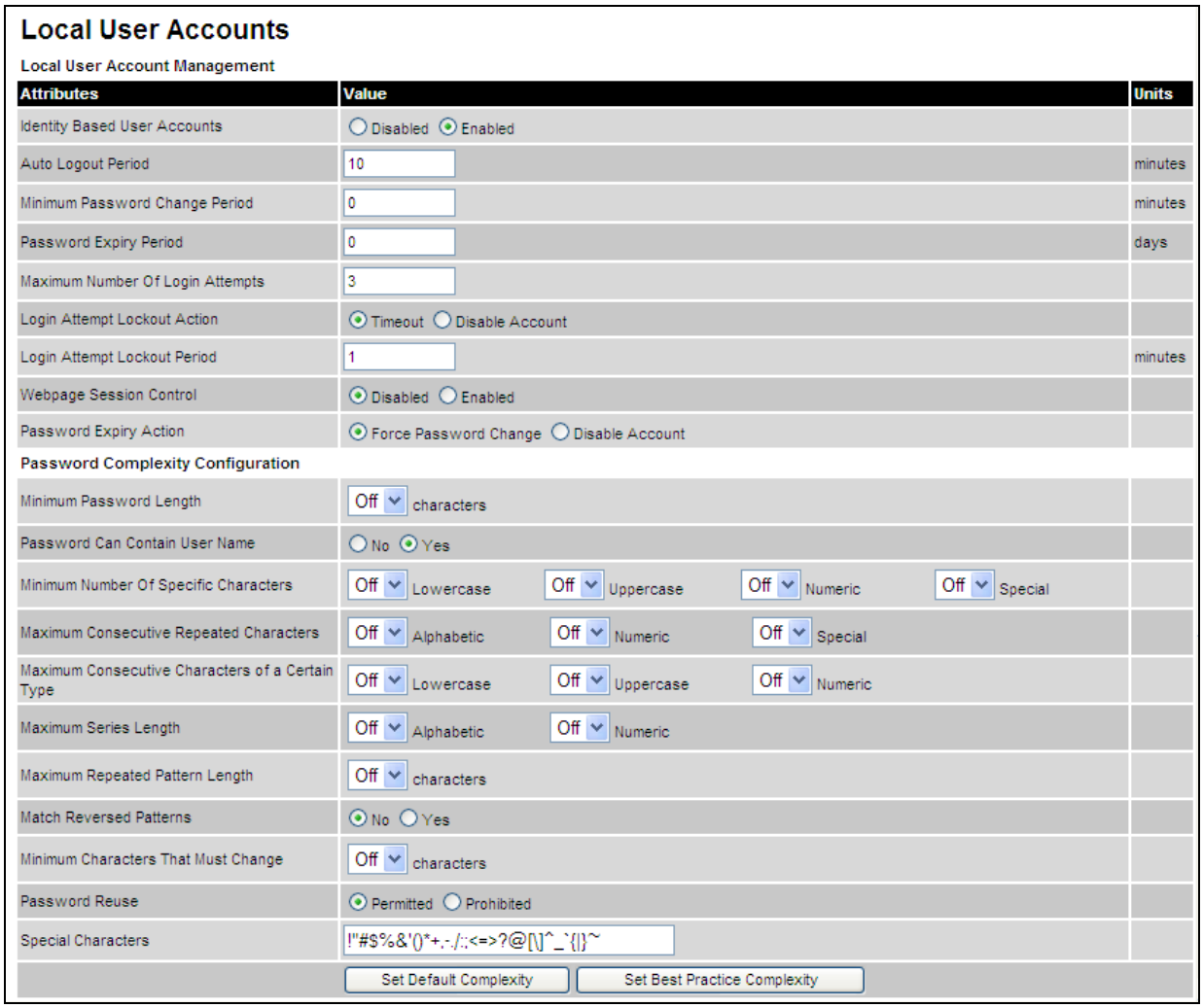
Perform this procedure to ensure that user access to the web-based management interface is controlled in accordance with the network operator's security policy.

If identity-based user accounts are enabled, this procedure may only be performed by a Security Officer.

Setting user account options

To set user account options, select menu option **Management, Web, Local User Accounts**. The Local User Accounts page is displayed (Figure 131). Review and update the Local User Account Management attributes (Table 227). If any attributes have been updated, select **Submit User Account Updates**.

Figure 131 Local User Accounts page (identity-based user accounts not shown)



Local User Accounts

Local User Account Management

Attributes	Value	Units
Identity Based User Accounts	○ Disabled ◉ Enabled	
Auto Logout Period	10	minutes
Minimum Password Change Period	0	minutes
Password Expiry Period	0	days
Maximum Number Of Login Attempts	3	
Login Attempt Lockout Action	◉ Timeout ○ Disable Account	
Login Attempt Lockout Period	1	minutes
Webpage Session Control	◉ Disabled ○ Enabled	
Password Expiry Action	◉ Force Password Change ○ Disable Account	
Password Complexity Configuration		
Minimum Password Length	Off characters	
Password Can Contain User Name	○ No ◉ Yes	
Minimum Number Of Specific Characters	Off Lowercase Off Uppercase Off Numeric Off Special	
Maximum Consecutive Repeated Characters	Off Alphabetic Off Numeric Off Special	
Maximum Consecutive Characters of a Certain Type	Off Lowercase Off Uppercase Off Numeric	
Maximum Series Length	Off Alphabetic Off Numeric	
Maximum Repeated Pattern Length	Off characters	
Match Reversed Patterns	◉ No ○ Yes	
Minimum Characters That Must Change	Off characters	
Password Reuse	◉ Permitted ○ Prohibited	
Special Characters	!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~	
	Set Default Complexity Set Best Practice Complexity	

Table 227 Local User account management attributes

Attribute	Meaning
Identity Based User Accounts	'Disabled' means that access to the web interface is controlled by a single system administration password. 'Enabled' means that the identity-based user account attributes are enabled. For more information, refer to Creating or updating identity-based users on page 6-47.
Auto Logout Period	The time without user activity that elapses before a user is automatically logged out (minutes).
Minimum Password Change Period	The minimum time that elapses before a user is allowed to change a password (minutes). A value of zero disables this feature.
Password Expiry Period	The time that elapses before a password expires (days). A value of zero disables this feature.
Maximum Number of Login Attempts	The maximum number of login attempts (with incorrect password) that are allowed before a user is locked out. Also, the maximum number of password change attempts before a user is locked out.
Login Attempt Lockout Action	Action to be taken when a user is locked out. 'Timeout' means the user is allowed to attempt to log in again after a specified period. 'Disabled' means the user is disabled.
Login Attempt Lockout Period	The time that elapses before a locked out user is allowed to log in again (minutes). Only displayed when Login Attempt Lockout Action is set to 'Timeout'.
Webpage Session Control	'Enabled' means that any attempt to open a new tab or browser instance will force the user to re-enter password.
Password Expiry Action	The action to be taken by the PTP 800 when a password expires.

Setting password complexity

Complete this task to configure password complexity rules for the web-based management interface. If identity-based user accounts are enabled, this task may only be performed by a Security Officer.

> **NOTE**
> If the unit is required to operate in FIPS 140-2 secure mode, set password complexity configuration to 'Best Practise Values'.

To set these options, proceed as follows:

1. Select menu option **Management, Web, Local User Accounts**. The Local User Accounts page is displayed (Figure 131).
2. Review and update the password complexity configuration attributes (Table 228).
3. To reset all attributes to the best practice values (as shown in Table 228), select **Set Best Practice Complexity**. This is required for FIPS 140-2.
4. To restore default values, select **Set Default Complexity**.
5. If any attributes have been updated, select **Submit User Account Updates**.

Table 228 Password complexity configuration attributes

Attribute	Meaning	Best practice
Minimum Password Length	The minimum number of characters required in passwords.	10
Password Can Contain User Name	'No' means that passwords must not contain the user name. 'Yes' means that passwords may contain the user name.	No
Minimum Number Of Specific Characters	The minimum number of lowercase, uppercase, numeric and special characters required in passwords. For example, if all values are set to 2, then 'FredBloggs' will be rejected, but 'FredBloggs(25)' will be accepted.	2

Attribute	Meaning	Best practice
Maximum Consecutive Repeated Characters	The maximum number of consecutive repeated alphabetic, numeric and special characters permitted in passwords. For example, if all values are set to 2, then ‘aaa’, ‘XXX’, ‘999’ and ‘$$$’ will be rejected, but ‘aa’, ‘XX’, ‘99’ or ‘$$’ will be accepted.	2
Maximum Consecutive Characters of a Certain Type	The maximum number of consecutive lowercase, uppercase and numeric characters permitted in passwords. For example, if all values are set to 5, then ‘ALFRED’, ‘neuman’ and ‘834030’ will be rejected.	5
Maximum Series Length	The maximum number of alphabetic and numeric characters permitted in passwords. For example, if set to 3, then ‘abcd’, ‘WXYZ’ and ‘0123’ will be rejected, but ‘abc’, ‘xyz’ and ‘123’ will be accepted.	3
Maximum Repeated Pattern Length	The maximum sequence of characters that can be repeated consecutively in passwords. For example, if set to 3, then ‘BlahBlah’ and ‘31st31st’ will be rejected, but ‘TicTicTock’ and ‘GeeGee’ will be accepted. ‘Blah-Blah’ will be accepted because the two sequences are not consecutive.	3
Match Reversed Patterns	‘No’ means that reversed patterns are not checked. ‘Yes’ means that reversed patterns are checked. For example, if Maximum Repeated Pattern Length is set to 3 and Match Reversed Patterns is set to ‘Yes’, then ‘AB1221BA’ will be rejected.	Yes
Minimum Characters That Must Change	The minimum number of password characters that must change every time a password is updated.	4
Password Reuse	‘Permitted’ means that a user may reuse a previous password. ‘Prohibited’ means that a user must not reuse a previous password.	Prohibited

Attribute	Meaning	Best practice
Special Characters	User defined set of special characters used in password construction. The only characters permitted in a password are: (a-z), (A-Z), (0-9) and any of the special characters entered here.	!"%&'()*+,-./:;<=>?

Creating or updating identity-based users

Perform this task to allow multiple users (from one to ten) to access the CMU with different levels of access. There are three defined levels of access: Security Officer, System Administrator and Read Only. If identity-based user accounts are already enabled, this task may only be performed by a user with role set to Security Officer.

To create or update identity-based user accounts, proceed as follows:

1. Select menu option **Management, Web, Local User Accounts**. The Local User Accounts page is displayed (Figure 131).
2. Set the Identity Based User Accounts attribute to 'Enabled' (if it is not already set). The identity-based user account attributes are enabled for update (Figure 132).
3. Create or update up to 10 user accounts (Table 229).
4. To restore default accounts, select **Reset to Factory Defaults**.
5. If any accounts have been created or updated, select **Submit User Account Updates**.

Figure 132 Identity-based user accounts

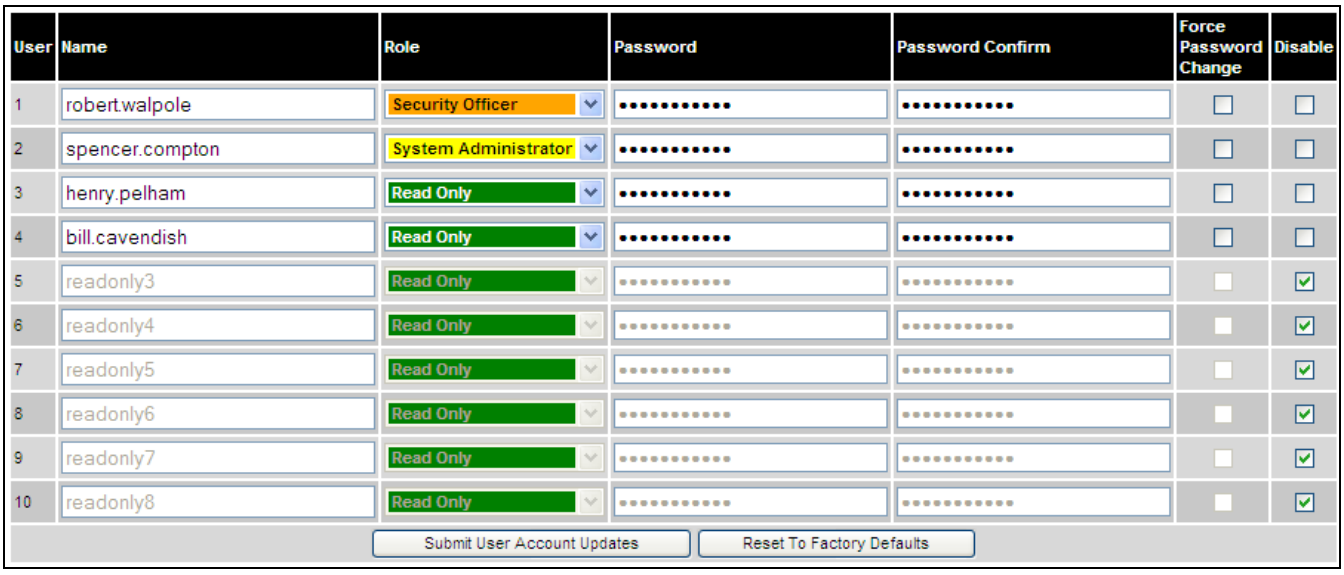


Table 229 Identity-based user accounts attributes

Attribute	Meaning
Name	Enter a user name.
Role	Select a role from the list: Security Officer System Administrator Read Only **NOTE** At least one user must be assigned the Security Officer role. If RADIUS is enabled, then this rule is relaxed, in which case the RADIUS server(s) SHOULD be configured with at least one user with 'Security Officer' privileges.
Password	Enter a password for the user. Passwords must comply with the complexity rules (Table 228).
Password Confirm	Retype the password to confirm.
Force Password Change	Force this user to change their password when they next log on.
Disable	Tick the box to disable a user account.

Changing own user password

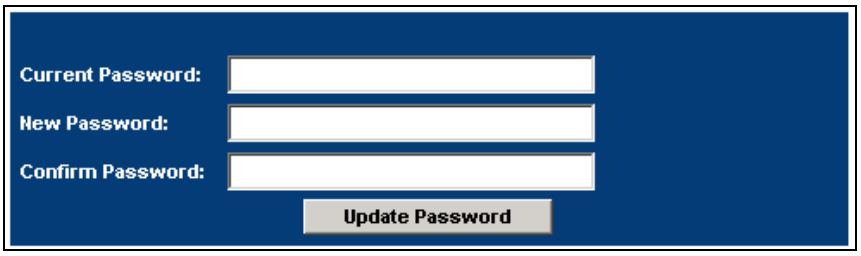
NOTE

This method may be used by any user to change their personal password.

A security officer can change the passwords of other users using the User Accounts page, as described in Creating or updating identity-based users on page 6-47.

Select menu option **Change Password**. The Change Password page is displayed (Figure 133). Enter and confirm the new password (the factory default is blank). The new password must comply with the complexity rules (Table 228).

Figure 133 Change Password page



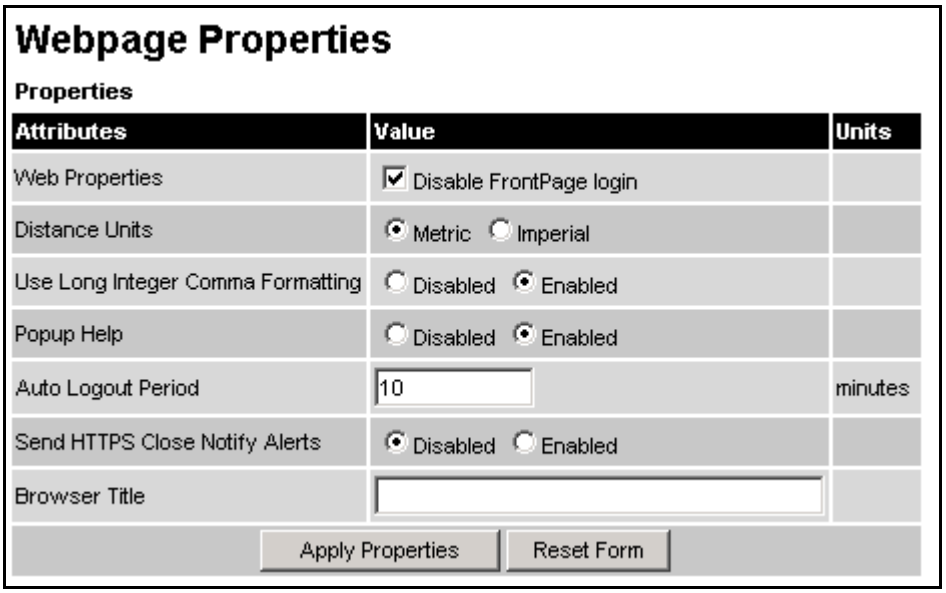
Protecting access to the summary and status pages

By default, the Home and Status menu items are not protected by password. If a higher level of system security is required, then apply password protection to these pages.

To apply password access to the System Summary and System Status pages, select menu option **Management, Web, Web Properties**. The Webpage Properties page is displayed (Figure 134). In the Web Properties attribute, uncheck the 'Disable FrontPage login' box and select **Apply Properties**.

If the System Administration Password has not yet been set, see Changing own user password on page 6-48.

Figure 134 Webpage Properties page



Configuring RADIUS authentication

This task is only performed when the PTP 800 link requires RADIUS authentication.

RADIUS authentication is only available when PTP 800 is configured for Identity-based User Accounts and when RADIUS servers are connected to the network.

Only users with 'Security Officer' role are permitted to configure RADIUS authentication.

NOTE

When RADIUS is enabled, the Security Officer may disable all local user accounts, as described in Creating or updating identity-based users on page 6-47.

NOTE

At least one user with Security Officer privileges must exist and be enabled, in order to disable the RADIUS client.

To configure RADIUS, select menu option **Management, Web, Radius Config**. The RADIUS Authentication page is displayed (Figure 135). Update the attributes as required (Table 230). Select **Submit RADIUS Configuration**.

Figure 135 RADIUS Configuration page

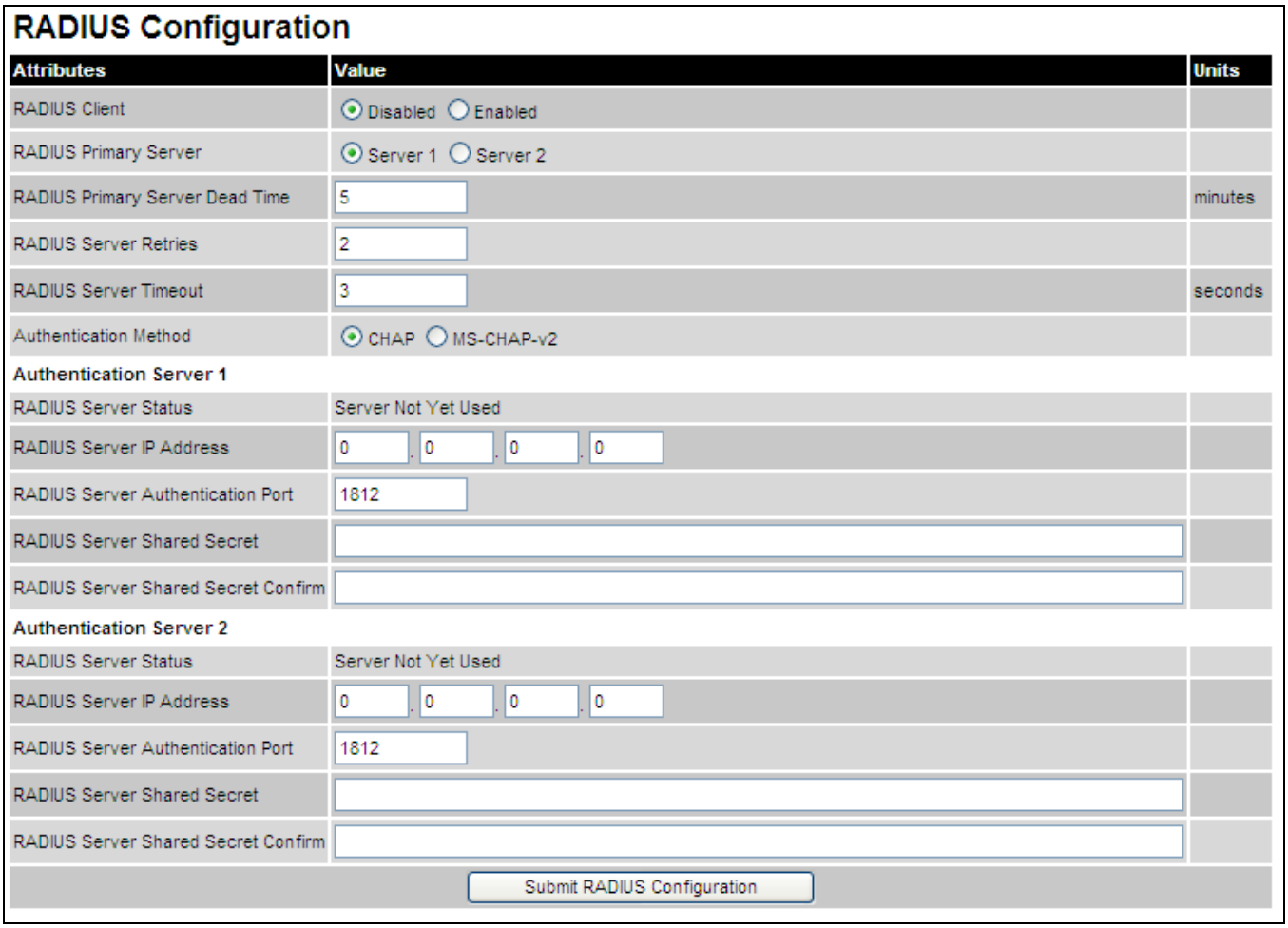


Table 230 RADIUS Authentication attributes

Attribute	Meaning
RADIUS Client Enabled	'Enabled' means that PTP 800 users may be authenticated via the RADIUS servers. 'Disabled' may only be selected if at least one user with Security Officer privileges exists.
RADIUS Primary Server	Specifies the primary server, determining the order in which the servers are tried.
RADIUS Primary Server Dead Time	Time (in minutes) to hold off trying to communicate with a previously unavailable RADIUS server. Setting the value to zero disables the timer.
RADIUS Server Retries	Number of times the PTP 800 will retry after a RADIUS server fails to respond to an initial request.
RADIUS Server Timeout	Time (in seconds) the PTP 800 will wait for a response from a RADIUS server.
Authentication Method	Method used by RADIUS to authenticate users.
Authentication Server 1 and 2:	
RADIUS Server Status	The status of the RADIUS server. This contains the time of the last test and an indication of success or failure. If the Authentication Server attributes are incorrect, the displayed status is 'server config not valid'.
RADIUS Server IP Address	IP address of the RADIUS server.
RADIUS Server Authentication Port	Network port used by RADIUS server for authentication services.
RADIUS Server Shared Secret	Shared secret used in RADIUS server communications. May contain alphabetic, numeric, special characters or spaces, but not extended unicode characters. The maximum length is 127 characters.
RADIUS Server Shared Secret Confirm	Shared secret confirmation.

Task 6: Configuring protection

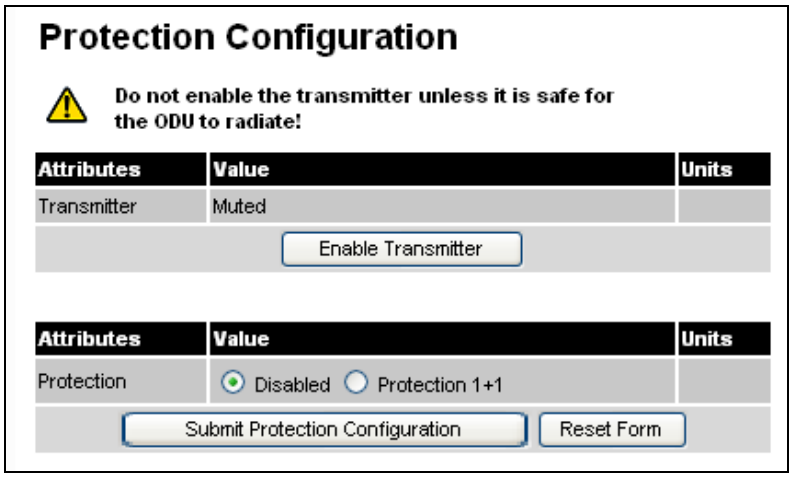
If the PTP 800 link is to be unprotected (1+0 or 2+0), perform Configuring unprotected links on page 6-53. If the PTP 800 link is to be protected using the 1+1 Hot Standby feature, perform Configuring 1+1 Hot Standby links on page 6-54.

To upgrade an existing unprotected link to use the 1+1 Hot Standby, perform Upgrading an unprotected link to 1+1 Hot Standby on page 6-61.

Configuring unprotected links

To ensure that protection is disabled, select menu option **System**, **Configuration, Protection**. When the Protection Configuration page is displayed (Figure 136), confirm that the Protection attribute is set to 'Disabled'.

Figure 136 Protection Configuration page (protection disabled)



The Status page shows details of the PTP 800 at the other end of the link with no protection information.

Configuring 1+1 Hot Standby links

Before configuring CMUs which are part of a 1+1 Hot Standby link, attach labels to each CMU specifying IP Address, Site Name and Primary or Secondary status. Make it very clear which site is required to transmit on the High side of the FDD frequency plan and which is required to transmit at the low side.

Depending on the configuration, a CMU labelled Primary must eventually be connected to one of the following:

- The ODU which is connected to the arm of the coupler labelled Main.
- The ODU which is connected to the antenna with the highest gain.
- The left hand transceiver in an IRFU.

For background information, see 1+1 Hot Standby link protection on page 1-64.

Before configuring the CMUs, ensure that the following information is known.

- Which CMU is to be configured as Primary and which unit is to be configured as Secondary. This is controlled by the Primary Secondary Mode attribute.
- Whether the end is to be installed with one or two antennas. This is controlled by the Number of Antennas attribute.
- Whether the method of connection to the Ethernet switch is via Fiber-Y. This is controlled by the Fiber-Y attribute. (see Network configurations for 1+1 on page 2-43 for details about Fiber-Y).
- Whether the Primary Recovery feature should be enabled and if so, the value of Primary Recovery Period. If the Primary has become Inactive for any reason, for example a previous fault, this feature automatically forces the Primary to become active again if it has been fault free for a configurable period of time defined by the Primary Recovery Period. This only needs to be configured on the CMU configured as Secondary.
- Whether an Ethernet port down alert is required on each protection switch. This is controlled by the Protection Switch Alert attribute. Enabling this feature is only of benefit in complex networks, for example where a 1+1 Hot Standby link forms part of a ring network architecture. This should normally remain disabled.
- Whether Receive Diversity is to be enabled (see Planning for Receive Diversity on page 2-46 for planning of this feature). This is controlled by the protection attribute.
- If Receive Diversity is to be enabled, ensure that the values for the Rx Diversity TPID (Tag Protocol Identifier) and the Rx Diversity VID (VLAN identifier) are known.

Before upgrading existing links from unprotected to protected, complete the following prerequisites:

- Configure the new CMUs as primary or secondary units by setting the Primary Secondary Mode attribute.
- For a new primary CMU, ensure that wireless transmission is disabled by selecting Mute Transmitter. This prevents possible interference with the existing operational unit.
- Attach ‘Primary” or ‘Secondary’ labels as appropriate to the new CMUs.
- Set Fault Protection Switching to ‘Disabled’. This prevents fault protection switches occurring during installation.

To configure protection, proceed as follows:

1. Select menu option **System, Configuration, Protection**. The Protection Configuration page is displayed (Figure 136).
2. If the Transmitter attribute is set to ‘Enabled’, there may be a safety requirement to disable wireless transmission. If so, select Mute Transmitter. The Transmitter attribute changes to ‘Muted’.
3. Depending on whether Receive Diversity is required, set the Primary unit protection attribute to either ‘Hot Standby 1+1’ (Figure 137) or ‘Hot Standby 1+1 with Rx Diversity’ (Figure 138).
4. Repeat at the Secondary unit (Figure 139 or Figure 140):
5. Review and update the Protection Configuration attributes (Table 231).
6. Select **Submit Updated configuration**.

Figure 137 Protection Configuration page for 1+1 (Primary)

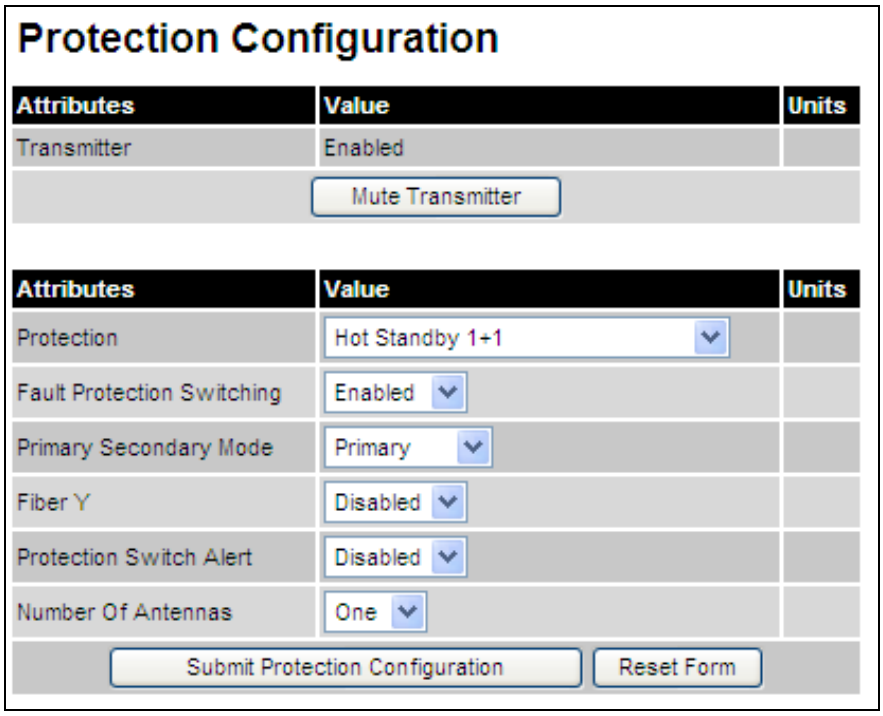


Figure 138 Protection Configuration page for 1+1 with Rx Diversity (Primary)

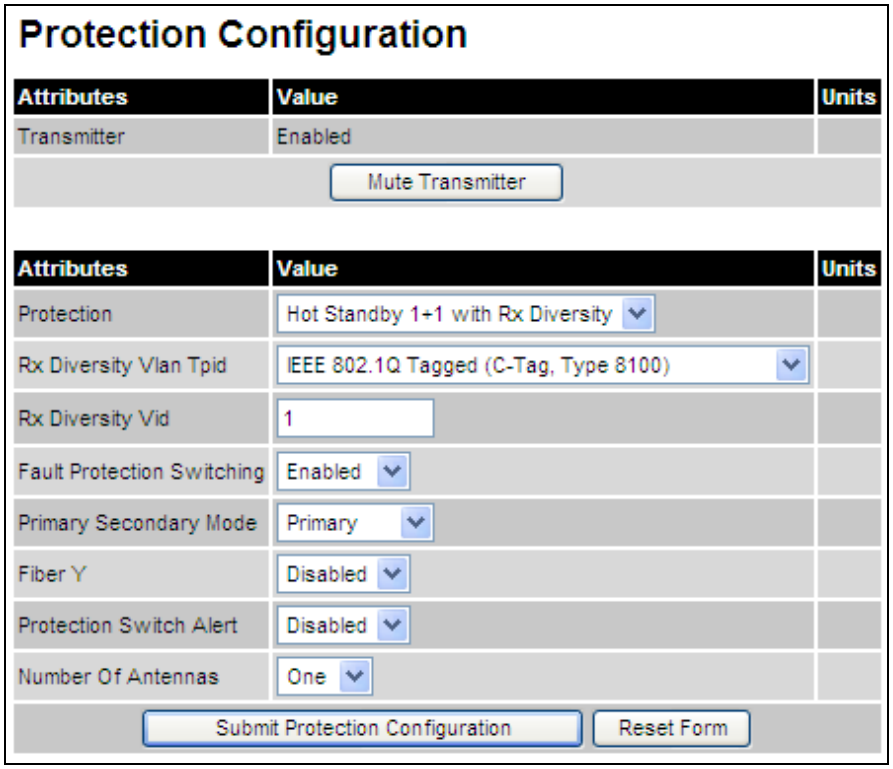


Figure 139 Protection Configuration page for 1+1 (Secondary)

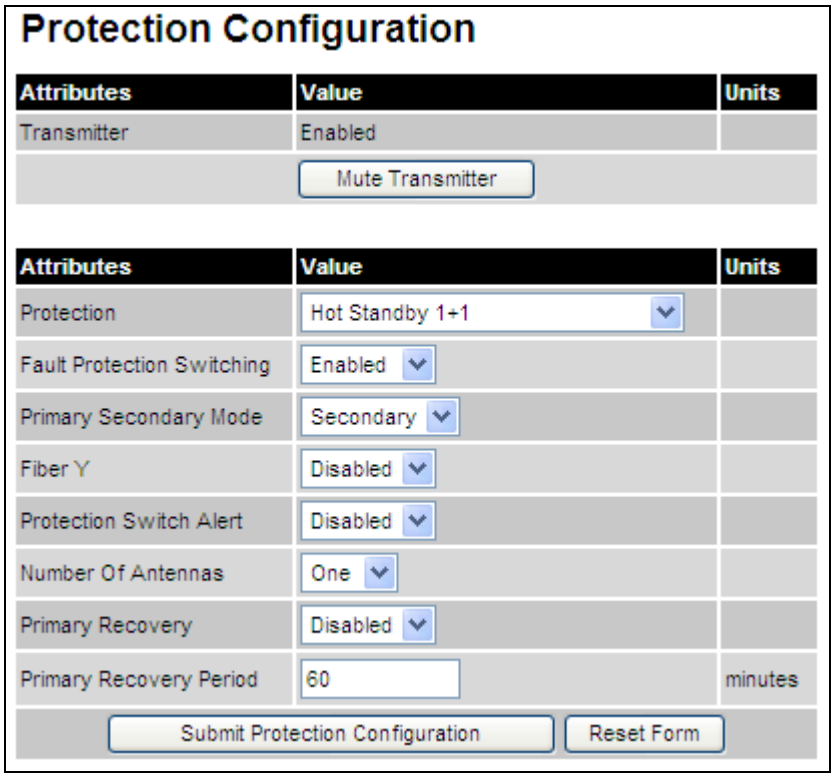
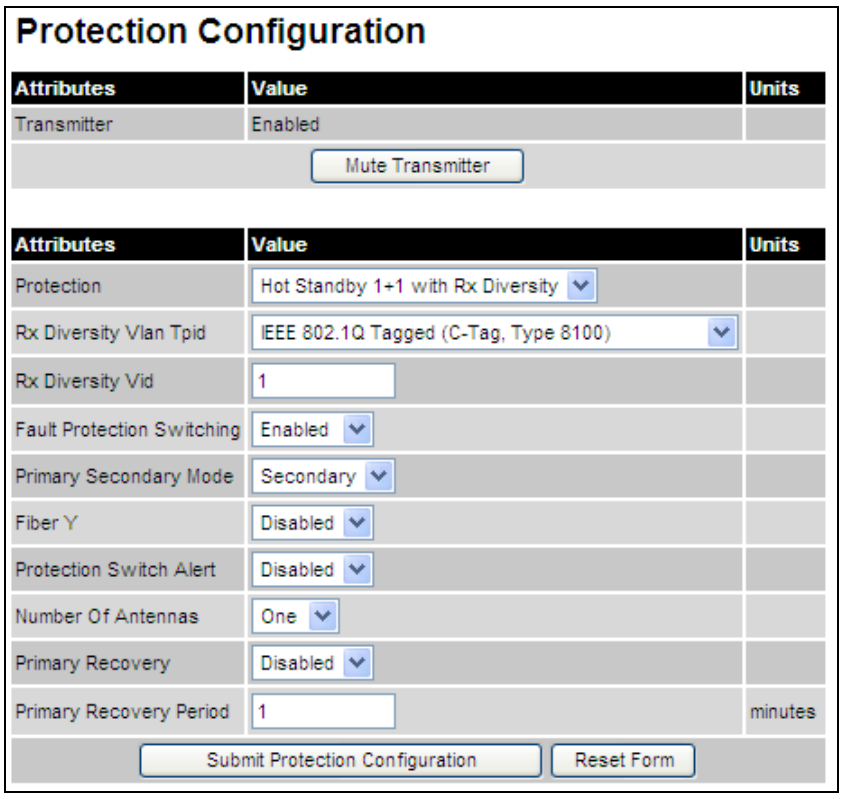


Figure 140 Protection Configuration page for 1+1 with Rx Diversity (Secondary)



NOTE

If a coupler is used, connect the Primary CMU to the ODU on the MAIN side of the coupler. This is especially important for an asymmetric coupler where the performance of the MAIN unit will be enhanced. In this case, set Primary Recovery Period to a non-zero value to maximize the use of the Main Path.

NOTE

If antenna protection is used and the two antennas are not the same, connect the Primary CMU to the more powerful antenna. In this case, for optimum link performance, Primary Recovery Period must also be set to a non-zero value.

Table 231 Protection Configuration attributes

Attribute	Meaning
Transmitter	'Muted' means that the RFU will not radiate and the CMU will not forward Ethernet frames between the wireless interface and the Ethernet ports. This applies in all conditions. 'Enabled' means that the RFU is allowed by the user to radiate and the CMU is allowed by the user to forward Ethernet frames between the wireless interface and the Ethernet ports. However, other factors may still prevent this, for example if the unit is the inactive unit at an end of a 1+1 Hot Standby link. **NOTE** This attribute does not indicate whether the unit is actually radiating and forwarding Ethernet Frames, but is a configuration attribute allowing the unit to radiate and forward traffic if other factors permit. To see if the unit is actually radiating and forwarding traffic, examine the Transmitter Status attribute on the Status page.
Protection	'Hot Standby 1+1' means that the link is protected. 'Hot Standby 1+1 with Rx Diversity' means that the link is protected and Receive Diversity is enabled. 'Disabled' means that the link is not protected.

Attribute	Meaning
Fault Protection Switching	'Enabled' means that normal 1+1 operation is in force. 'Disabled' means that a protection switch will not occur when a fault is detected on the active unit. With this setting, the user still has the ability to change which unit is active. This setting can be useful during installation or maintenance operations where the user wishes to have full control of which unit is active. When this is set to 'Enabled', a protection switch will occur when a fault is detected on the active unit.
Primary Secondary mode	The CMU is configured as a Primary or Secondary. The Primary is the preferred unit, meaning that it is the active unit unless it is faulty. If the two ODUs at an end have a different path loss, for example where they are coupled to a common antenna using an Asymmetric Coupler Mounting Kit (see Coupler mounting kits on page 1-30), connect the CMU configured as Primary to the RFU with the lowest path loss.
Fiber-Y	'Enabled' means that the neighboring CMUs at the end of a 1+1 Hot Standby link are connected to the network via a Fiber-Y interface (see Installing a Fiber-Y interface on page 5-93). 'Disabled' means that a Fiber-Y interface is not installed. **NOTE** If a CMU is being replaced in an otherwise working 1+1 Hot Standby link, do not connect the Fiber-Y cable to the CMU until this attribute is enabled. If the Fiber-Y cable is connected before enabling this attribute, the 1+1 link will not transmit customer data.
Number of Antennas	The number of antennas to be installed at this end of the link.

Attribute	Meaning
Primary Recovery	Only available when Primary Secondary mode is set to 'Secondary'. 'Enabled' means that when the Secondary unit is active, the Primary unit is only allowed to become active if it has been fault free for a configurable period of time.
Primary Recovery Period	Only available when Primary Secondary mode is set to 'Secondary'. How long (in mutes) the Primary unit must be free of faults before it is allowed to take over as the active unit (see Primary Recovery).
Protection Switch Alert	'Enabled' means that the CMU will alert the Ethernet switch when a protection switch has occurred. The CMU issues this alert by briefly (between 0.5 and 1 second) disabling the Ethernet port on the newly active unit. For most network deployments this is set to 'Disabled'. Setting this to 'Enabled' may however be useful in complex networks where the network design is to allow an alternative route to bridge the traffic following a protection switch.
Rx Diversity TPID	The Inactive unit sends special Receive Diversity Ethernet Frames to the Active unit via the Ethernet Switch. These frames must be configured to be tagged as either C-TAG or S-TAG frames.
Rx Diversity VID	The Inactive unit sends special Receive Diversity Ethernet Frames to the Active unit via the Ethernet Switch. These frames must be configured with a specific VID.

Upgrading an unprotected link to 1+1 Hot Standby

This section describes how to upgrade an existing unprotected link to use the 1+1 Hot Standby link protection feature.

CAUTION

Although the disruption to an existing link can be minimized, this process cannot be carried out without interrupting the operation of the link.

The following actions will interrupt link operation:

- Upgrading the software. This can be carried out in advance of hardware installation. Alternatively during the installation after the inactive units have been installed and when the inactive units are providing an operational link, the existing units may be upgraded and configured.
- Installing a second ODU on the coupler if a single antenna is used at each end.
- Aligning antennas when antenna protection is implemented. As the new antennas operate on the same frequencies as the existing ones, alignment cannot be performed while the existing antennas run an operational link.
- Other operations if working close to an antenna.
- Testing that the protection is working correctly by forcing protection switchovers.

NOTE

If configuration is carried out on site, then before the new units are taken to site, radio transmission should be inhibited as described in Disabling wireless transmission on page 7-32. This prevents possible interference with the existing operational unit.

To implement protection on an unprotected link, follow this process:

1. To pre-configure the two new CMUs during staging before site installation (if this is required), perform the following tasks from Chapter 6: Configuration and alignment for each CMU:

   from Task 1: Connecting to the unit on page 6-3,
   to Task 11: Configuring remote access on page 6-96.

   Perform these tasks after installation, if preferred.

2. In the field, upgrade the operational CMUs to the latest software version by performing Task 4: Upgrading software version on page 6-25.

3. In the field, configure the operational CMUs for protected operation by performing Task 6: Configuring protection on page 6-53.

   > **NOTE**
   > If this is done in advance of installation of the new CMUs, the PTP 800 will still be operational and the wireless link can operate with single units, but alarms will be issued due to the absence of protecting units.

   The Protected link page is now available with local and remote ends shown as unprotected, see Viewing the status of a 1+1 Hot Standby link on page 7-33.

4. Install and test the new hardware by following the relevant procedures in this chapter.

5. Align the antennas and complete the configuration. Perform the following tasks from Chapter 6: Configuration and alignment:

   from Task 12: Aligning antennas on page 6-98,
   to Task 15: Connecting link to the network on page 6-114.

6. Initiate a protection switch so that the link is running Primary to Primary. If primary recovery is set, the units will switch automatically after the timer has expired.

Task 7: Configuring wireless interface

The Installation Wizard handles the important configuration settings that must be set to comply with the individual license conditions. These settings can only be changed using the Installation Wizard.

This task consists of the following procedures:

- Prerequisites for the Installation Wizard on page 6-63
- Step 1: Enter equipment details on page 6-65
- Step 2: Enter details of the radio license on page 6-69
- Step 3: Configuring wireless parameters on page 6-72
- Step 4: Confirming installation configuration on page 6-73
- Step 5: Skipping antenna alignment on page 6-75
- Step 6: Completing configuration without alignment on page 6-76

Prerequisites for the Installation Wizard

Before performing Steps 1 to 4 of the Installation Wizard, check that the following are available:

- All license details, including maximum EIRP, antenna gain, transmit and receive frequencies, channel bandwidth.
- A unique link name for this link.

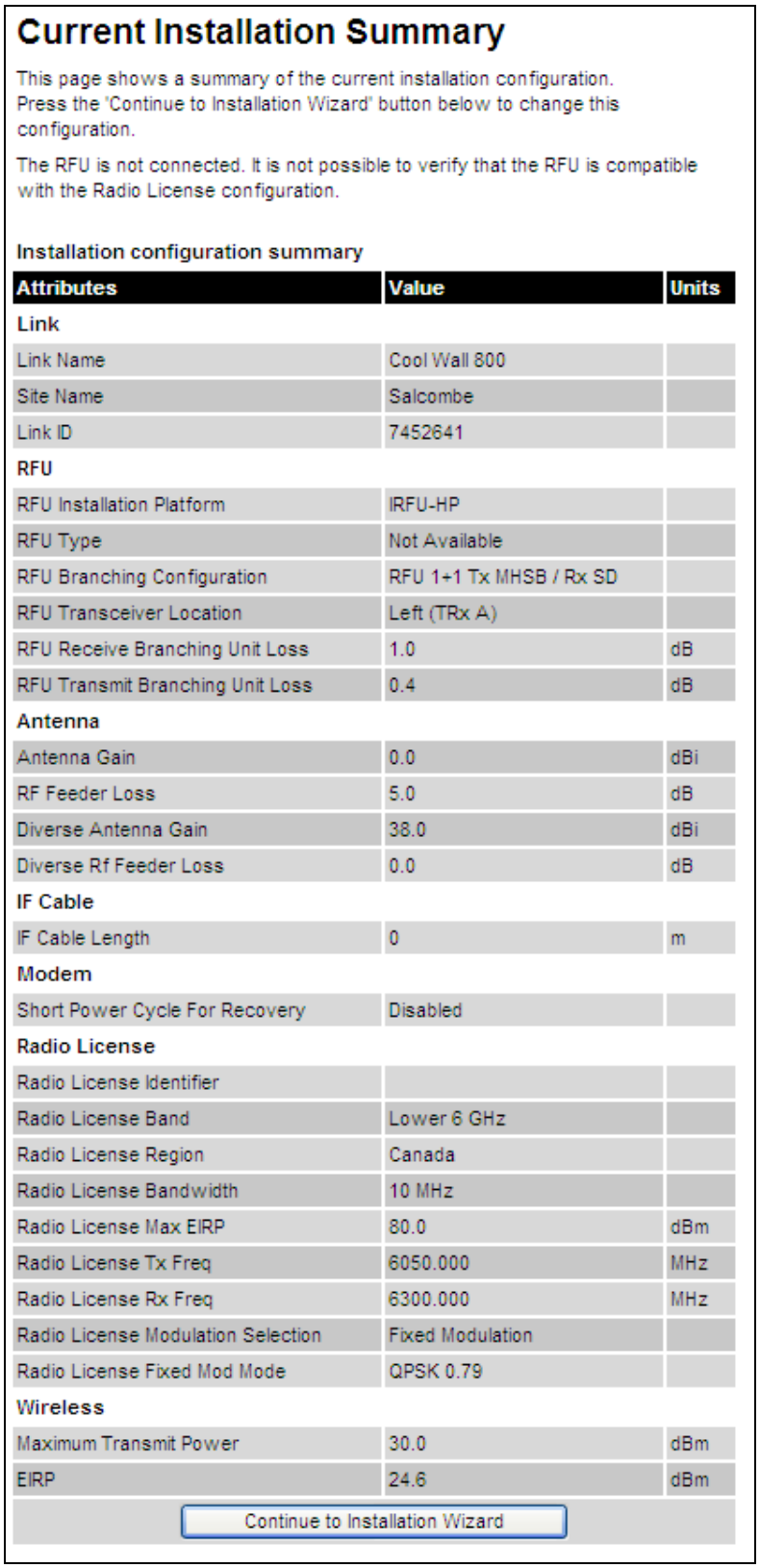
⚠ CAUTION

Link Name must be the same at both link ends, otherwise the link will not work.

Starting Installation Wizard

To start the Installation Wizard, select menu option **Installation**. The Current Installation Summary page (Figure 141) is displayed. Review the summary. To make any changes, select **Continue to Installation Wizard**.

Figure 141 Current Installation Summary page



Current Installation Summary

This page shows a summary of the current installation configuration. Press the 'Continue to Installation Wizard' button below to change this configuration.

The RFU is not connected. It is not possible to verify that the RFU is compatible with the Radio License configuration.

Installation configuration summary

Attributes	Value	Units
Link		
Link Name	Cool Wall 800	
Site Name	Salcombe	
Link ID	7452641	
RFU		
RFU Installation Platform	IRFU-HP	
RFU Type	Not Available	
RFU Branching Configuration	RFU 1+1 Tx MHSB / Rx SD	
RFU Transceiver Location	Left (TRx A)	
RFU Receive Branching Unit Loss	1.0	dB
RFU Transmit Branching Unit Loss	0.4	dB
Antenna		
Antenna Gain	0.0	dBi
RF Feeder Loss	5.0	dB
Diverse Antenna Gain	38.0	dBi
Diverse Rf Feeder Loss	0.0	dB
IF Cable		
IF Cable Length	0	m
Modem		
Short Power Cycle For Recovery	Disabled	
Radio License		
Radio License Identifier		
Radio License Band	Lower 6 GHz	
Radio License Region	Canada	
Radio License Bandwidth	10 MHz	
Radio License Max EIRP	80.0	dBm
Radio License Tx Freq	6050.000	MHz
Radio License Rx Freq	6300.000	MHz
Radio License Modulation Selection	Fixed Modulation	
Radio License Fixed Mod Mode	QPSK 0.79	
Wireless		
Maximum Transmit Power	30.0	dBm
EIRP	24.6	dBm

Continue to Installation Wizard

Step 1: Enter equipment details

Step 1 of the Installation Wizard is for updating the equipment configuration. If RFU Installation Platform is 'ODU-A' or 'ODU-B', the page is displayed without IRFU attributes (Figure 142). If RFU Installation Platform is 'IRFU-HP', the page is displayed with IRFU attributes (Figure 143). The attributes are described in Table 232. Update the attributes as required and select **Next**.

Figure 142 Step 1: Enter equipment details page (ODU)

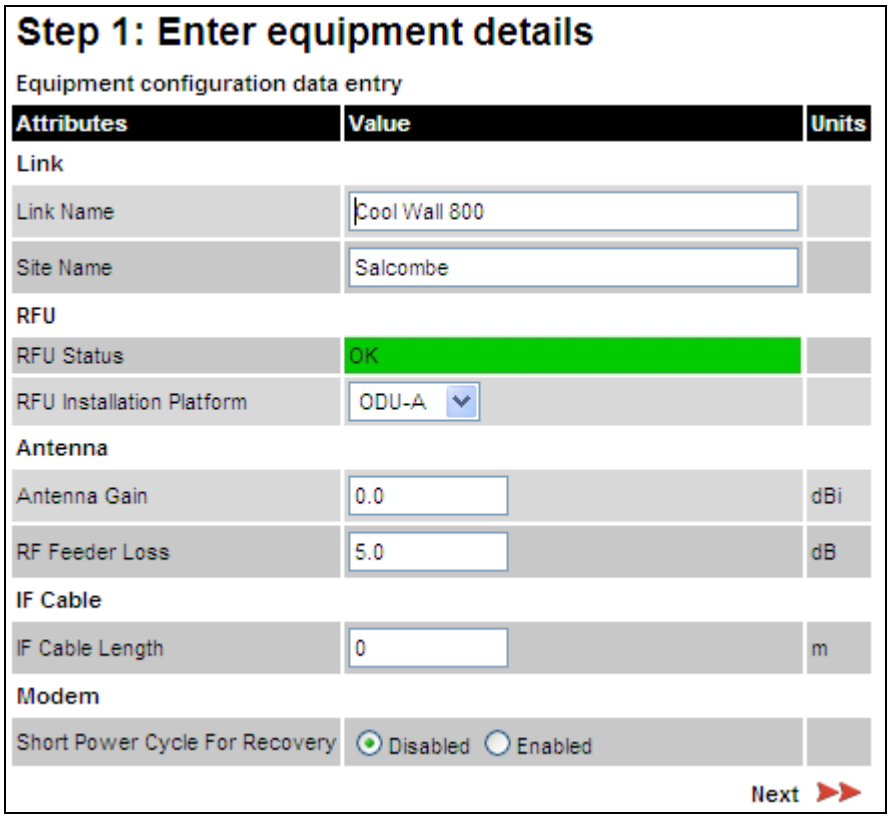


Figure 143 Step 1: Enter equipment details page (IRFU)

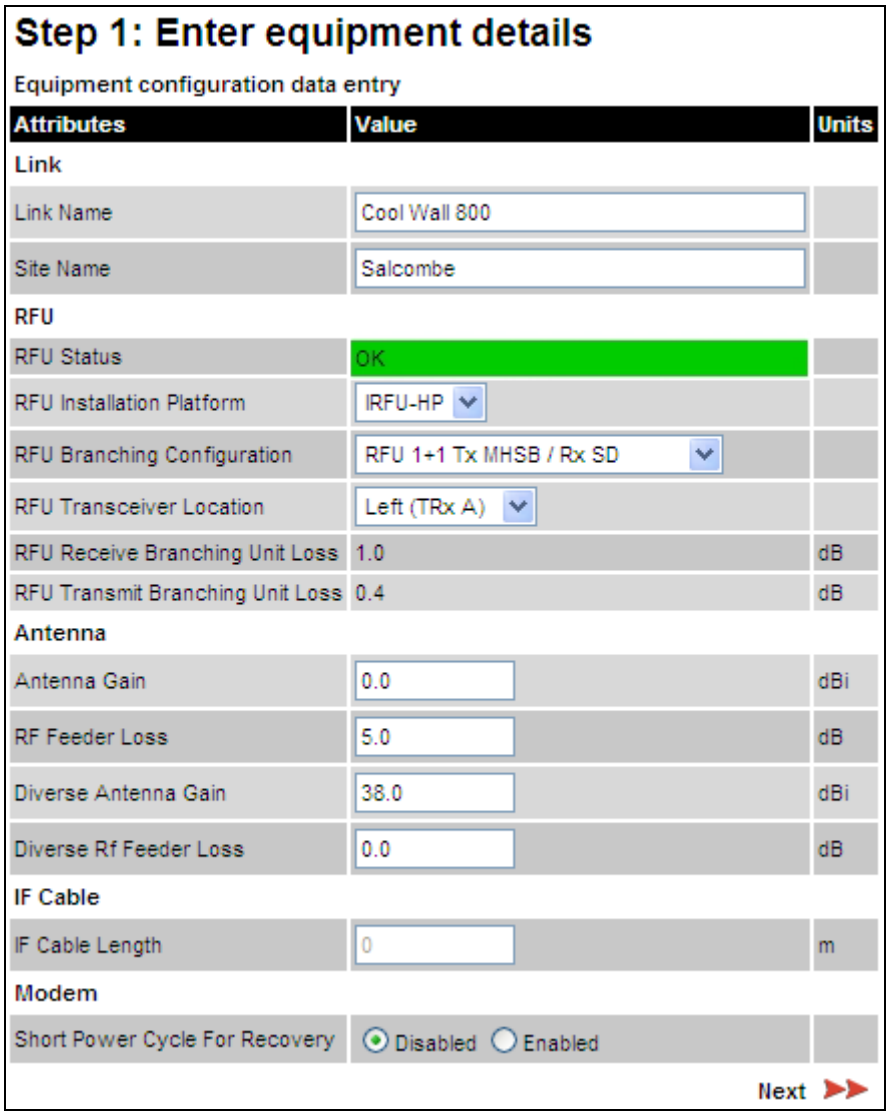


Table 232 Step 1: Equipment Configuration attributes

Attribute	Meaning
Link	
Link Name	A meaningful name for the PTP link. It is used to establish a connection with the PTP 800 at the other link end (site). **NOTE** Ensure that Link name is the same at both ends of the link. If the Link name is not the same, the link will not establish.

Attribute	Meaning
Site Name	The Site Name where the unit is to be installed. **NOTE** For 1+1 Hot Standby links, it is recommended that the Primary and Secondary CMUs installed at the same end are configured with the same Site Name. An individual unit within a network is then identifiable from the three attributes: Link Name, Site Name and Primary Secondary Mode.
RFU	
RFU Status	The status of the RFU. If the RFU is not connected to the CMU, this attribute indicates “No Response” with a red background.
RFU Installation Platform	The type of RFU installed. If an RFU is already connected, the CMU detects and identifies the type, and this attribute cannot be changed. If no RFU is connected, this attribute can be pre-set to show the RFU platform that will be installed (IRFU-HP, ODU-A or ODU-B).
RFU Branching Configuration	Only displayed when RFU Installation Platform is set to ‘IRFU-HP’. The required IRFU branching configuration: RFU 1+0 RFU 1+0 MHSB Ready (Equal) RFU 1+0 MHSB Ready (Unequal) RFU 1+1 MHSB (Equal) RFU 1+1 MHSB (Unequal) RFU 1+1 Tx MHSB / Rx SD RFU 2+0
RFU Transceiver Location	Only displayed when RFU Installation Platform is set to ‘IRFU-HP’ and RFU Branching Configuration is not ‘RFU 1+0’. The CMU must know the location of the transceiver within the IRFU to which it is connected: Left (TRx A) Right (TRx B)

Attribute	Meaning
RFU Receive Branching Unit Loss	Only displayed when RFU Installation Platform is set to 'IRFU-HP'. The receiver branching unit loss between the IRFU waveguide port and the transceiver.
RFU Transmit Branching Unit Loss	Only displayed when RFU Installation Platform is set to 'IRFU-HP'. The transmitter branching unit loss between the transceiver and IRFU waveguide port.
Antenna	
Antenna Gain	The gain (dBi) of the main antenna.
RF Feeder Loss	The loss (dB) in the feeder (waveguide) between the RFU and antenna, including loss of couplers. This should be zero for a direct mount configuration with no coupler. Waveguide specifications are provided in Flexible waveguide specifications on page 4-10.
Diverse Antenna Gain	Only displayed when RFU Installation Platform is set to 'IRFU-HP' and RFU Branching Configuration is set to 'RFU 1+1 Tx MHSB / Rx SD'. The gain (dBi) of the diverse antenna.
Diverse RF Feeder Loss	Only displayed when RFU Installation Platform is set to 'IRFU-HP' and RFU Branching Configuration is set to 'RFU 1+1 Tx MHSB / Rx SD'. The loss (dB) in the feeder (waveguide) between the IRFU and diverse antenna.
IF Cable	
IF Cable Length	The total length of the IF cable from the RFU to the CMU in meters or feet as appropriate. The maximum permitted length is 190 meters (620 ft) for standard IF cable. **NOTE** If the IF cable length is between 190 and 300 meters (620 ft and 980 ft), contact Technical Support. The units can be changed using the Properties web page.
Modem	

Attribute	Meaning
Short Power Cycle For Recovery	'Enabled' means that a short power cycle will cause the CMU to boot in recovery mode. This is the better option when the CMU is installed in a location that is difficult to access. 'Disabled' means that the CMU will boot in recovery mode only through use of the front panel recovery switch. This is the better option when it is reasonably easy to access the CMU to press the Recovery button. For more information, see Using recovery mode on page 7-71.

Step 2: Enter details of the radio license

Step 2 of the Installation Wizard is for updating radio license attributes (Figure 144 or Figure 145 or Figure 146). The attributes are described in Table 233. Update the attributes as required and select **Next**.

Figure 144 Step 2: Radio License Configuration page (fixed modulation)

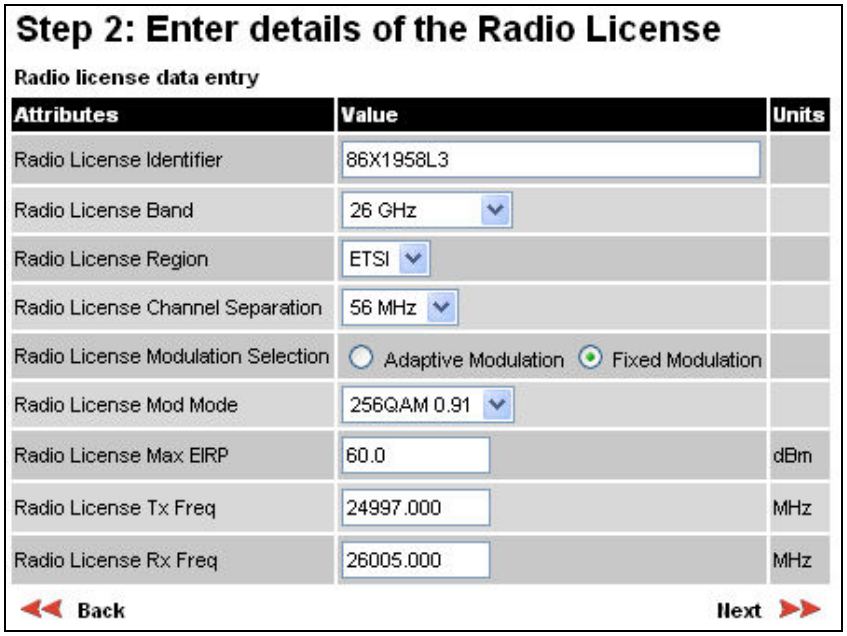


Figure 145 Step 2: Radio License Configuration page (FCC adaptive modulation)

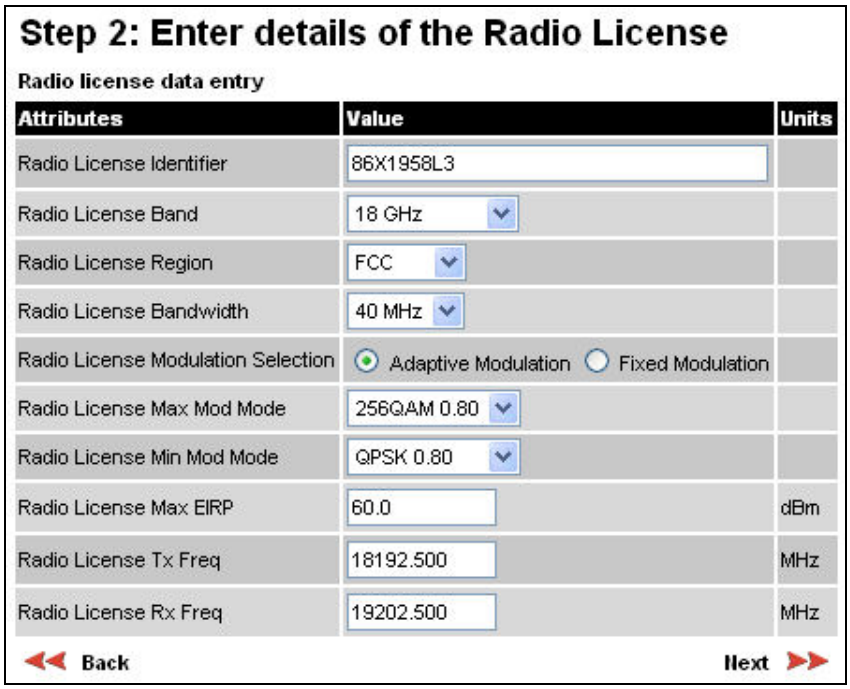


Figure 146 Step 2: Radio License Configuration page (ETSI adaptive modulation)

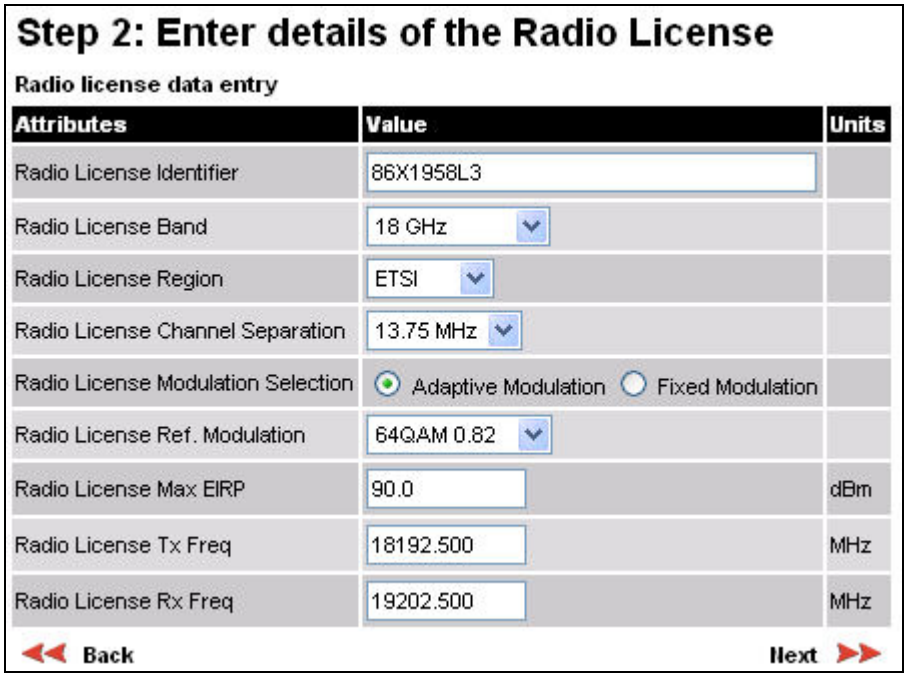


Table 233 Step 2: Radio License Configuration attributes

Attribute	Meaning
Radio License Identifier	An identifier for the radio license, for example a certificate number, if one was provided by the licensing authority. This attribute is for reference only.
Radio License Band	The licensed band (GHz). When an RFU is attached, this attribute is set automatically.
Radio License Region	The license region.
Radio License Bandwidth	The licensed bandwidth (MHz). This attribute is only displayed when Radio License Region is set to FCC or Canada.
Radio License Channel Separation	The licensed spacing between channels (MHz). This attribute is only displayed when Radio License Region is set to ETSI or Brazil.
Radio License Modulation Selection	'Fixed Modulation' is the default. 'Adaptive Modulation' may be available, if permitted by the license.
Radio License Mod Mode	The licensed modulation mode. This attribute is only displayed when Radio License Modulation Selection is set to 'Fixed Modulation'.
Radio License Ref. Modulation	Reference modulation mode specified by the license. This control is only visible for certain regions when Radio License Modulation Selection is set to 'Adaptive'.
Radio License Max Mod Mode	The highest modulation mode allowed by the license. This control is only visible for certain regions when Radio License Modulation Selection is set to 'Adaptive'.
Radio License Min Mod Mode	Select the lowest modulation mode allowed by the license. This control is only visible for certain regions when Radio License Modulation Selection is set to 'Adaptive'.
Radio License Max EIRP	The maximum permitted strength of the radio signal in dBm EIRP.
Radio License Tx Frequency	The licensed transmit frequency (MHz).
Radio License Rx Frequency	The licensed receive frequency (MHz).

Step 3: Configuring wireless parameters

Step 3 of the Installation Wizard is for updating the constraints on wireless operation (Figure 147 or Figure 148). The attributes are described in Table 234. Update the attributes as required and select **Next**.

Figure 147 Step 3: Wireless Configuration page (normal)

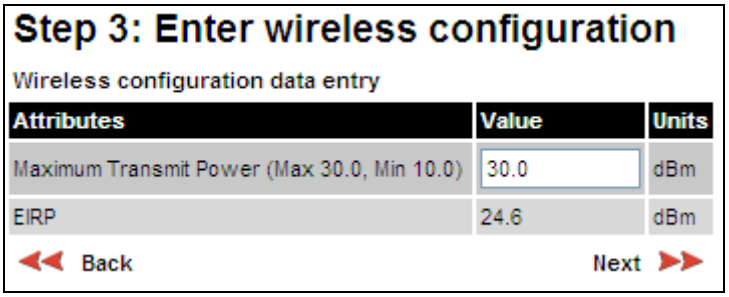


Figure 148 Step 3: Wireless Configuration page (ETSI adaptive modulation)

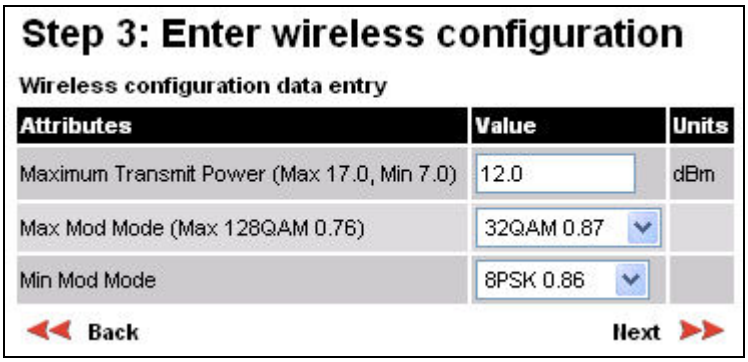


Table 234 Step 3: Wireless Configuration attributes

Attribute	Meaning
Maximum Transmit Power	The maximum transmit power the wireless unit is permitted to use when establishing and maintaining the wireless link. This defaults to the lowest of the maximum allowed by the equipment, the maximum allowed by the license or the user maximum set in a previous installation. **NOTE** When an IRFU is connected (rather than an ODU), this refers to the power at the transceiver output, not at the antenna port.
EIRP	EIRP that is achieved when the transmitter is operating at the configured Maximum Transmit Power.

Attribute	Meaning
User ACM Highest Mod Mode	The maximum modulation mode the radio can use when ACM is enabled. The valid range depends on the region, license and Tx Max Power. This attribute is only visible for certain regions when Radio License Modulation Selection is set to 'Adaptive'.
User ACM Lowest Mod Mode	The minimum modulation mode the radio can use when ACM is enabled. The valid range depends on the region, license and Tx Max Power. This attribute is only visible for certain regions when Radio License Modulation Selection is set to 'Adaptive'.

Step 4: Confirming installation configuration

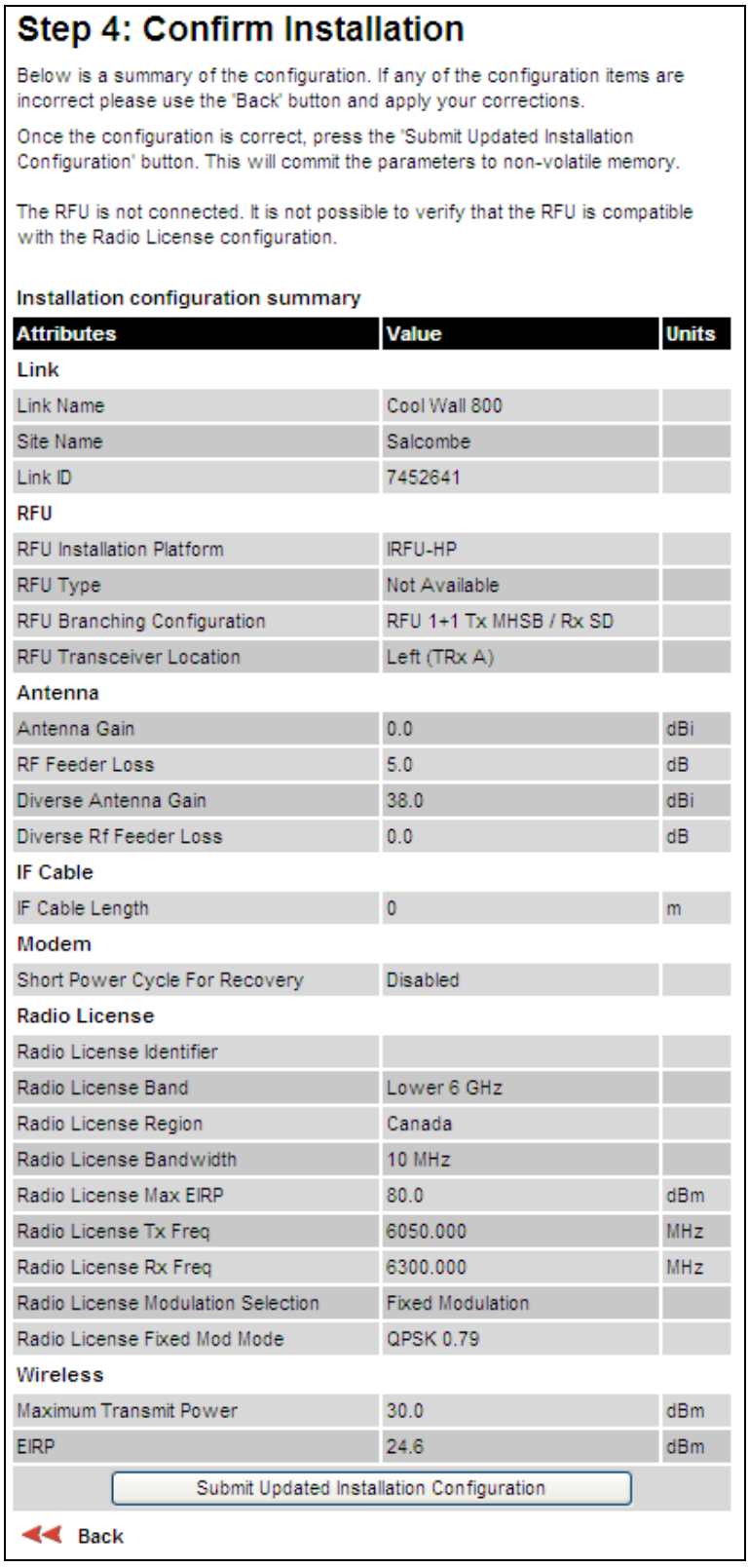
When the Step 4: Confirm Installation Configuration page is displayed (Figure 149), review the attributes. If any are incorrect, select **Back** and return to the appropriate step to correct them. If all attributes are correct, select **Submit Updated Installation Configuration** or **Next**.

NOTE

If the RFU is not connected to the CMU, the RFU Type attribute is set to 'Not Present'.

Changed parameters are shown in bold.

Figure 149 Step 4: Confirm Installation Configuration page



Step 4: Confirm Installation

Below is a summary of the configuration. If any of the configuration items are incorrect please use the 'Back' button and apply your corrections.

Once the configuration is correct, press the 'Submit Updated Installation Configuration' button. This will commit the parameters to non-volatile memory.

The RFU is not connected. It is not possible to verify that the RFU is compatible with the Radio License configuration.

Installation configuration summary

Attributes	Value	Units
Link		
Link Name	Cool Wall 800	
Site Name	Salcombe	
Link ID	7452641	
RFU		
RFU Installation Platform	IRFU-HP	
RFU Type	Not Available	
RFU Branching Configuration	RFU 1+1 Tx MHSB / Rx SD	
RFU Transceiver Location	Left (TRx A)	
Antenna		
Antenna Gain	0.0	dBi
RF Feeder Loss	5.0	dB
Diverse Antenna Gain	38.0	dBi
Diverse Rf Feeder Loss	0.0	dB
IF Cable		
IF Cable Length	0	m
Modem		
Short Power Cycle For Recovery	Disabled	
Radio License		
Radio License Identifier		
Radio License Band	Lower 6 GHz	
Radio License Region	Canada	
Radio License Bandwidth	10 MHz	
Radio License Max EIRP	80.0	dBm
Radio License Tx Freq	6050.000	MHz
Radio License Rx Freq	6300.000	MHz
Radio License Modulation Selection	Fixed Modulation	
Radio License Fixed Mod Mode	QPSK 0.79	
Wireless		
Maximum Transmit Power	30.0	dBm
EIRP	24.6	dBm

Submit Updated Installation Configuration

Back

Step 5: Skipping antenna alignment

WARNING

Do not start antenna alignment until it is safe for the antennas to radiate RF, that is, until the antennas and ODUs have been installed on the masts or poles and no personnel are in front of the antennas.

NOTE

If the Installation Wizard is being run during pre-configuration before site installation, then defer antenna alignment until site installation is complete at both link ends.

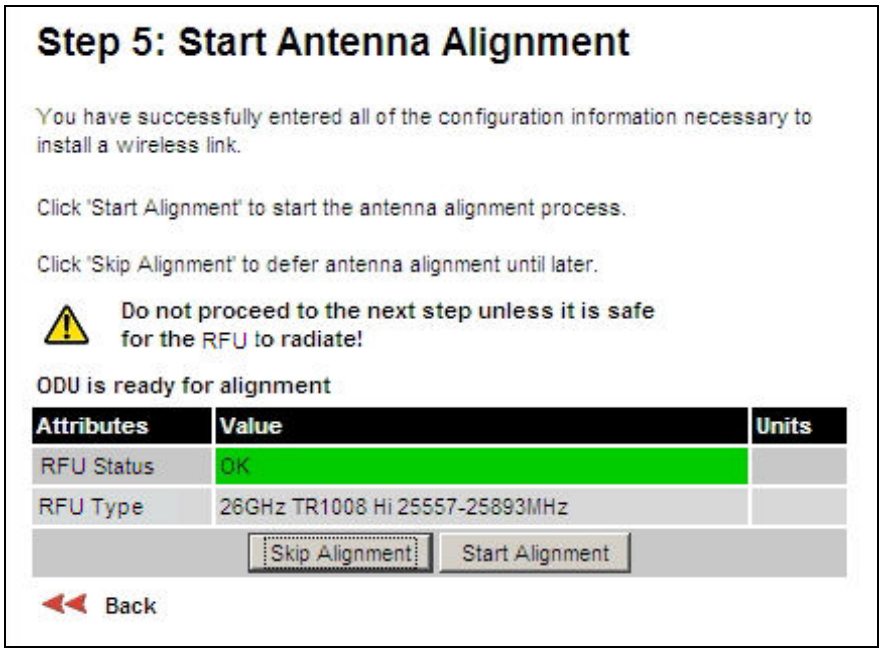
When the Step 5: Start Antenna Alignment page is displayed (Figure 150), choose whether to defer or start alignment:

- To defer alignment, select Skip Alignment. This cancels the Install Wizard without doing alignment, but configuration changes are saved.
- To start alignment, continue at Task 12: Aligning antennas on page 6-98.

NOTE

If the RFU is not connected to the CMU, then the **Start Alignment** option is disabled. The Installation Wizard does not allow progress to antenna alignment.

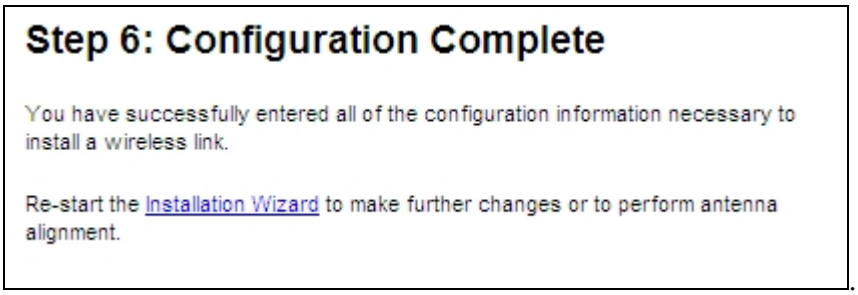
Figure 150 Step 5: Start Antenna Alignment page


Step 5: Start Antenna Alignment
You have successfully entered all of the configuration information necessary to install a wireless link.
Click 'Start Alignment' to start the antenna alignment process.
Click 'Skip Alignment' to defer antenna alignment until later.
Do not proceed to the next step unless it is safe for the RFU to radiate!
ODU is ready for alignment
Attributes
Value
Units
RFU Status
OK
RFU Type
26GHz TR1008 Hi 25557-25893MHz
Skip Alignment
Start Alignment
Back

Step 6: Completing configuration without alignment

The Step 6: Configuration Complete page is displayed (Figure 151). If the pre-configuration of the PTP 800 system is complete, then close the web interface.

Figure 151 Step 6: Configuration Complete page (step 5 cancelled)


Step 6: Configuration Complete
You have successfully entered all of the configuration information necessary to install a wireless link.
Re-start the Installation Wizard to make further changes or to perform antenna alignment.

Task 8: Setting up SNMP agent

If SNMP is enabled, when an event occurs, the SNMP agent on the unit sends a trap to whatever SNMP trap receivers have been configured.

Depending upon which SNMP version is required, choose one of the following procedures:

- Configuring SNMPv3 agent on page 6-77
- Configuring SNMPv1/2c agent on page 6-86

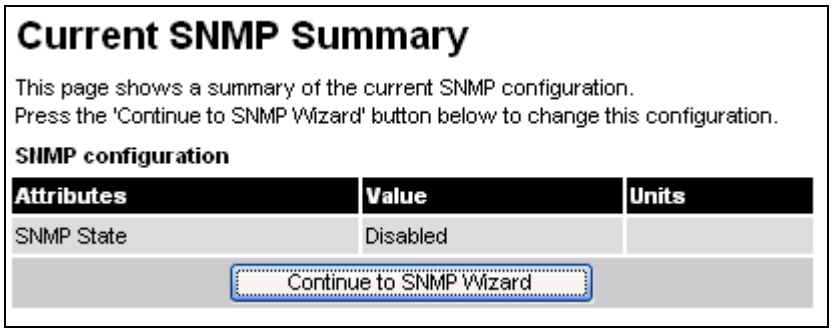
Configuring SNMPv3 agent

Perform this task to enable the system to generate Simple Network Management Protocol version 3 (SNMPv3) traps.

Starting SNMP wizard

To start the SNMP wizard, select menu option **Management, SNMP**. The Current SNMP Summary page is displayed (Figure 152). Review the summary. If any updates are required, select **Continue to SNMP Wizard**.

Figure 152 Current SNMP Summary page (when SNMP is disabled)



Step 1: SNMP configuration (for SNMPv3)

The Step 1: SNMP Configuration page is displayed. Set SNMP State to 'Enabled' and set SNMP Version to 'v3'. The page is redisplayed with SNMPv3 attributes (Figure 153). Update the attributes (Table 235), then select **Next**.

Figure 153 Step 1: SNMP Configuration page (for SNMPv3)

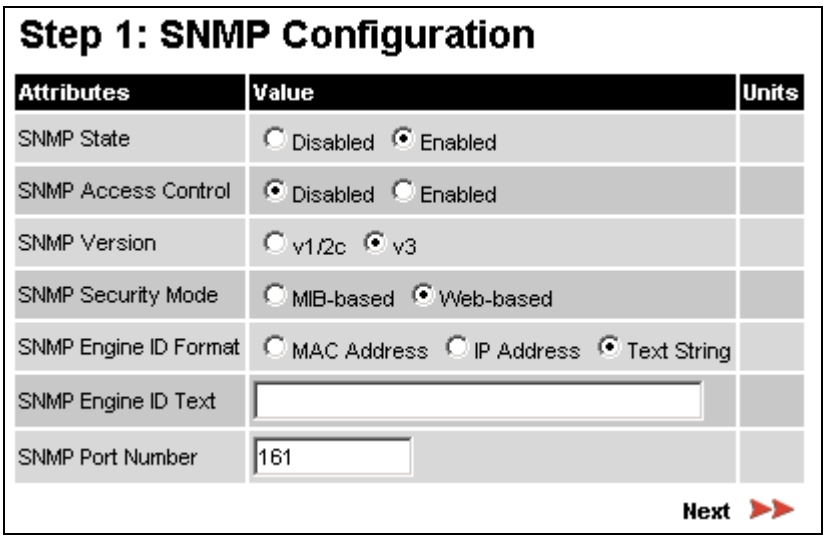


Table 235 Step 1: SNMP Configuration attributes (for SNMPv3)

Attribute	Meaning
SNMP State	'Enabled' means that the system will generate SNMP traps.
SNMP Access Control	'Enabled' means that access to SNMP is controlled via IP address. Up to three IP addresses may be entered.
SNMP Version	SNMP protocol version v1/2c or v3.
SNMP Security Mode	'MIB-based' means that SNMPv3 security parameters are managed via SNMP MIBs. 'Web-based' means that the SNMPv3 security parameters are not available over SNMP, but instead are configured using the SNMP Accounts page, as described in Step 3: SNMP user policy configuration (for SNMPv3) on page 6-79.
SNMP Engine ID Format	Specifies whether the Engine ID is generated from the MAC Address, IP Address or Text String.
SNMP Engine ID Text	Text used to generate the SNMP Engine ID.Only available when SNMP Engine ID Format is set to 'Text String'.

Attribute	Meaning
SNMP Port Number	The port that the SNMP agent monitors to detect commands from a management system.

Step 2: SNMP MIB-II system objects

The Step 2: SNMP MIB-II System Objects page is displayed (Figure 154). Update the attributes (Table 236), then select **Next**.

Figure 154 Step 2: SNMP MIB-II System Objects page

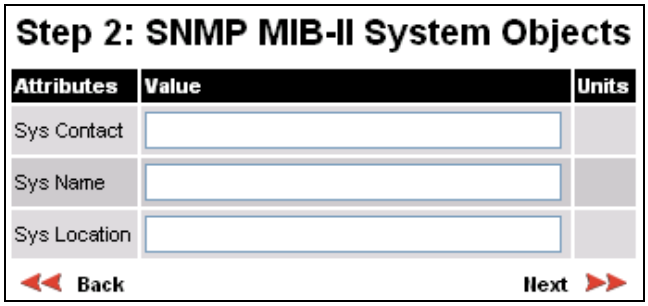


Table 236 Step 2: SNMP MIB-II System Objects attributes

Attribute	Meaning
Sys Contact	The contact name for this managed node, with contact details.
Sys Name	An administratively-assigned name for this managed node. By convention, this is the fully-qualified domain name.
Sys Location	The physical location of this node.

Step 3: SNMP user policy configuration (for SNMPv3)

If the chosen SNMP Security Mode is ‘Web-based’, the Step 3: SNMP User Policy Configuration page is displayed (Figure 155). Update the web-based security profile attributes (Table 237): these determine which authentication and privacy protocols are required for SNMP users with roles ‘System Administrator’ and ‘Read only’. Select **Next**.

Figure 155 Step 3: SNMP User Policy Configuration page (for SNMPv3)

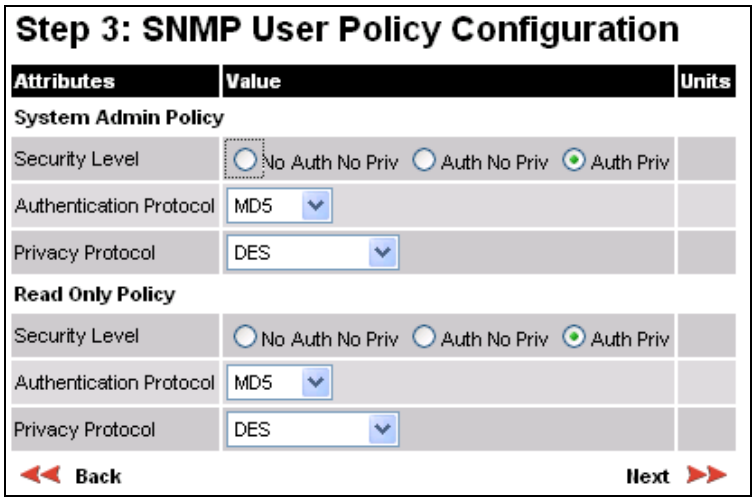


Table 237 Step 3: SNMP User Policy Configuration attributes (for SNMPv3)

Attribute	Meaning
Security Level	Defines the security level and associated protocols that are required to allow SNMP users to access the system. 'No Auth No Priv' means that users are not required to use authentication or privacy protocols. 'Auth No Priv' means that users are required to use only authentication protocols. 'Auth Priv' means that users are required to use both authentication and privacy protocols.
Authentication Protocol	The authentication protocol to be used to access the system via SNMP. This is disabled when Security Level is set to 'No Auth No Priv'. 'MD5' means Message Digest Algorithm. 'SHA' means NIST FIPS 180-1, Secure Hash Algorithm SHA-1.
Privacy Protocol	The privacy protocol to be used to access the system via SNMP. This is disabled when Security Level is set to 'No Auth No Priv' or 'Auth No Priv'. 'DES' means Data Encryption Standard (DES) symmetric encryption protocol. 'AES' means Advanced Encryption Standard (AES) cipher algorithm. **NOTE** A user configured to use AES privacy protocol will not be able to transmit and receive encrypted messages unless the license key enables the AES capability.

Step 4: SNMP user accounts configuration (for SNMPv3)

If the chosen SNMP Security Mode is 'Web-based', the Step 4: SNMP User Accounts Configuration page is displayed (Figure 156). Update the individual user attributes (Table 238) for up to 10 SNMP users, then select **Next**.

Figure 156 Step 4: SNMP User Accounts Configuration page (for SNMPv3)

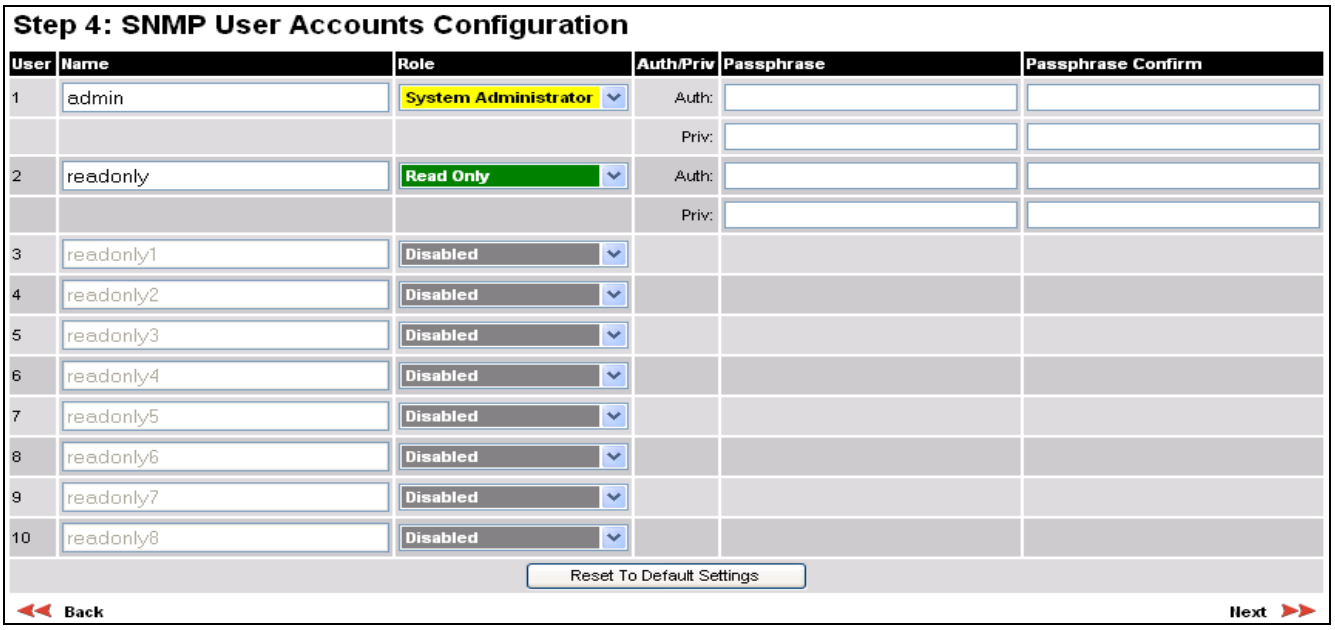


Table 238 Step 3: SNMP User Accounts Configuration attributes (for SNMPv3)

Attribute	Meaning
Name	Name to be used by the SNMP user to access the system.
Role	Selects which of the two web-based security profiles are applied to this user: 'System administrator' or 'Read only'. 'Disabled' means that the SNMP account is disabled.
Auth/Priv	Indicates whether the Passphrase applies to authentication or privacy protocols.
Passphrase	The phrase to be entered by this SNMP user to access the system using an authentication or privacy protocol. Length must be between 8 and 32 characters. May contain spaces. The 'Auth:' Passphrase is hidden when Security Level for this user's Role is set to 'No Auth No Priv'. The 'Priv:' Passphrase is hidden when Security Level for this user's Role is set to 'No Auth No Priv' or 'Auth No Priv'.

Attribute	Meaning
Passphrase Confirm	Confirmation of Passphrase, to detect mis-keying.

Step 5: SNMP trap configuration (for SNMPv3)

If the chosen SNMP Security Mode is 'Web-based', the Step 5: SNMP Trap Configuration page is displayed (Figure 157). Update the attributes (Table 239), then select **Next**.

Figure 157 Step 5: SNMP Trap Configuration page (for SNMPv3)

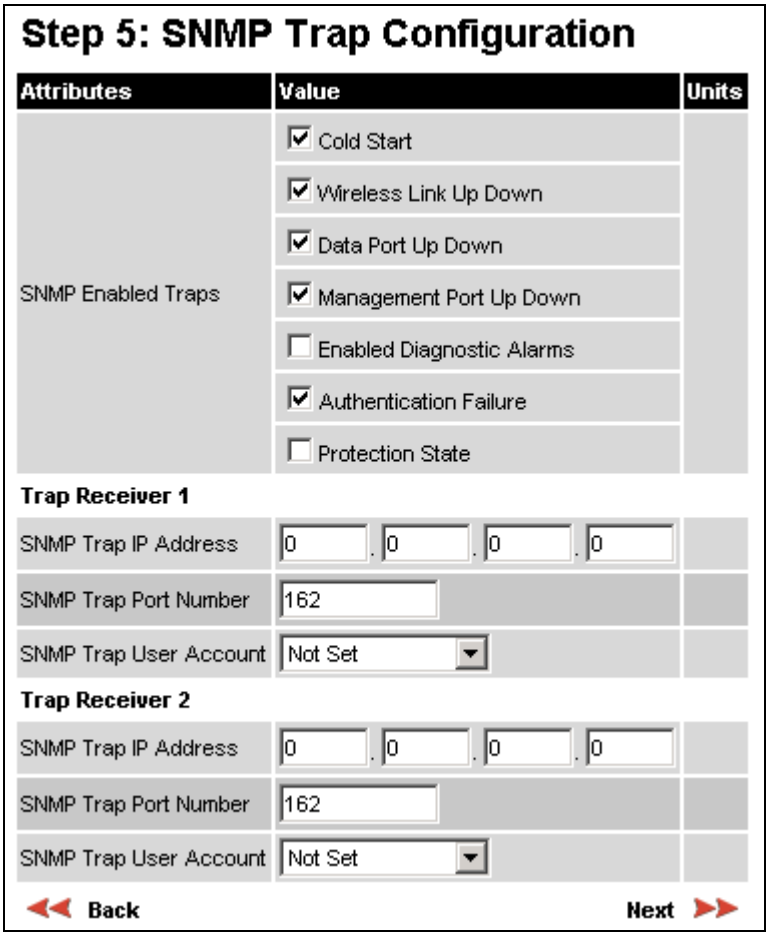


Table 239 Step 5: SNMP Trap Configuration attributes (for SNMPv3)

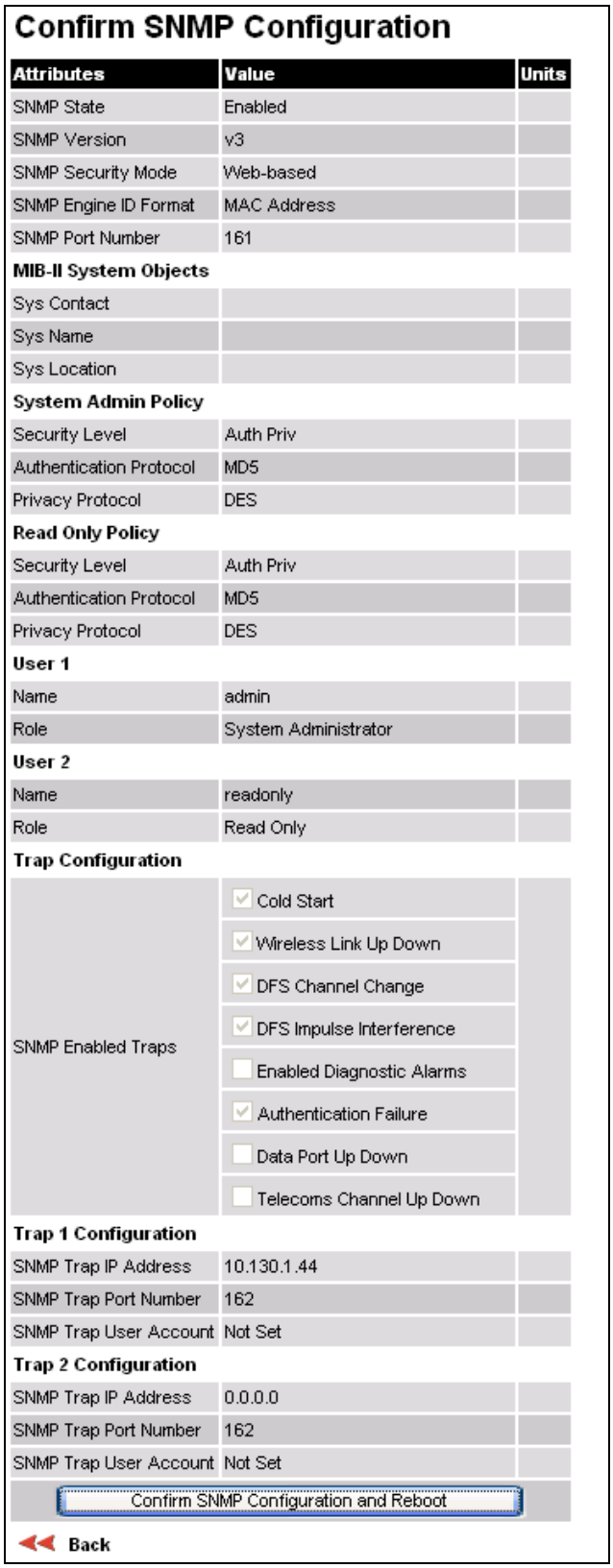
Attribute	Meaning
SNMP Enabled Traps	The events that will generate SNMP traps.

Attribute	Meaning
SNMP Trap IP Address 1	The IP address of the first SNMP server (trap receiver). This is normally the network management system, but it may be a separate trap receiver. A value of zeros disables logging on the first SNMP server.
SNMP Trap Port Number 1	The server 1 port at which SNMP traps are received.
SNMP Trap User Account 1	The user name (and associated protocols) to use when sending SNMP traps to server 1.
SNMP Trap IP Address 2	The IP address of the second SNMP server (trap receiver). This is normally the network management system, but it may be a separate trap receiver. A value of zeros disables logging on the second SNMP server.
SNMP Trap Port Number 2	The server 2 port at which SNMP traps are received.
SNMP Trap User Account 2	The user name (and associated protocols) to use when sending SNMP traps to server 2.

Confirming SNMP configuration (for SNMPv3)

When the Confirm SNMP Configuration page (Figure 158) is displayed, review the settings and select either **Back** or **Confirm SNMP Configuration and Reboot**. When the settings are confirmed, the unit reboots.

Figure 158 Confirm SNMP Configuration page (for SNMPv3)



Confirm SNMP Configuration

Attributes	Value	Units
SNMP State	Enabled	
SNMP Version	v3	
SNMP Security Mode	Web-based	
SNMP Engine ID Format	MAC Address	
SNMP Port Number	161	
MIB-II System Objects		
Sys Contact		
Sys Name		
Sys Location		
System Admin Policy		
Security Level	Auth Priv	
Authentication Protocol	MD5	
Privacy Protocol	DES	
Read Only Policy		
Security Level	Auth Priv	
Authentication Protocol	MD5	
Privacy Protocol	DES	
User 1		
Name	admin	
Role	System Administrator	
User 2		
Name	readonly	
Role	Read Only	
Trap Configuration		
SNMP Enabled Traps	☑ Cold Start	
	☑ Wireless Link Up Down	
	☑ DFS Channel Change	
	☑ DFS Impulse Interference	
	☐ Enabled Diagnostic Alarms	
	☑ Authentication Failure	
	☐ Data Port Up Down	
	☐ Telecoms Channel Up Down	
Trap 1 Configuration		
SNMP Trap IP Address	10.130.1.44	
SNMP Trap Port Number	162	
SNMP Trap User Account	Not Set	
Trap 2 Configuration		
SNMP Trap IP Address	0.0.0.0	
SNMP Trap Port Number	162	
SNMP Trap User Account	Not Set	

Confirm SNMP Configuration and Reboot

Back

Configuring SNMPv1/2c agent

Perform this task to enable the system to generate Simple Network Management Protocol version 1 or 2c (SNMPv1 or SNMPv2c) traps.

Start SNMP wizard

To start the SNMP wizard, select menu option **Management, SNMP**. The Current SNMP Summary page is displayed (Figure 152). Review the summary. If any updates are required, select **Continue to SNMP Wizard**.

Step 1: SNMP Configuration (for SNMPv1/2c)

The Step 1: SNMP Configuration page is displayed. Set SNMP State to 'Enabled' and set SNMP Version to 'v1/2c'. The page is redisplayed with SNMPv1/2c attributes (Figure 159). Update the attributes (Table 240), then select **Next**.

Figure 159 Step 1: SNMP Configuration page (for SNMPv1/2c)

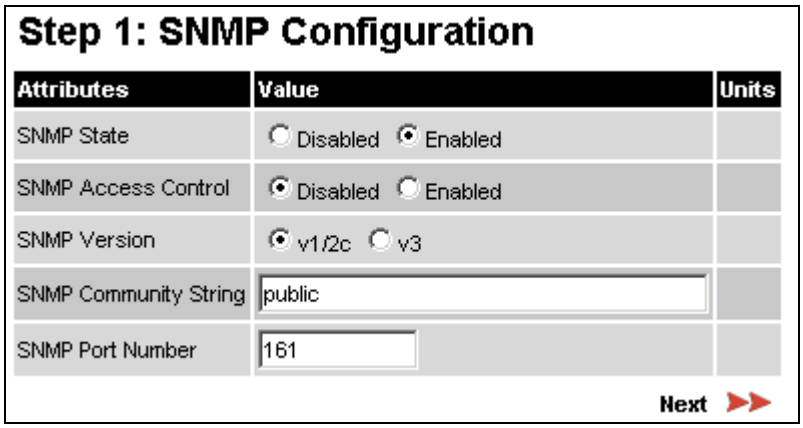


Table 240 Step 1: SNMP Configuration attributes (for SNMPv1/2c)

Attribute	Meaning
SNMP State	'Enabled' means that the system will generate SNMP traps.
SNMP Access Control	'Enabled' means that access to SNMP is controlled via IP address. Up to three IP addresses may be entered.
SNMP Version	SNMP protocol version v1/2c or v3.

Attribute	Meaning
SNMP Community String	The SNMP community string acts like a password between the network management system and the distributed SNMP clients (PTP 800 ODUs). Only if the community string is configured correctly on all SNMP entities can the flow of management information take place. By convention the default value is set to 'public'.
SNMP Port Number	The port that the SNMP agent is listening to for commands from a management system.

Step 2: SNMP MIB-II system objects

The Step 2: SNMP MIB-II System Objects page is displayed (Figure 154). Update the attributes (Table 236), then select **Next**.

Step 3: SNMP Trap Configuration (for SNMPv1/2c)

If the chosen SNMP Security Mode is 'MIB-based', the Step 5: SNMP Trap Configuration page is displayed (Figure 160). Update the attributes (Table 241), then select **Next**.

Figure 160 Step 3: SNMP Trap Configuration page (for SNMPv1/2c)

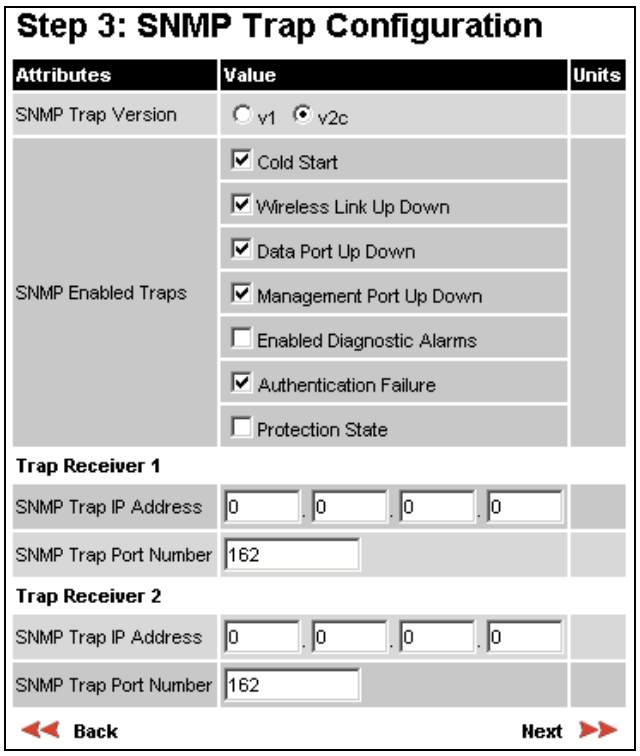


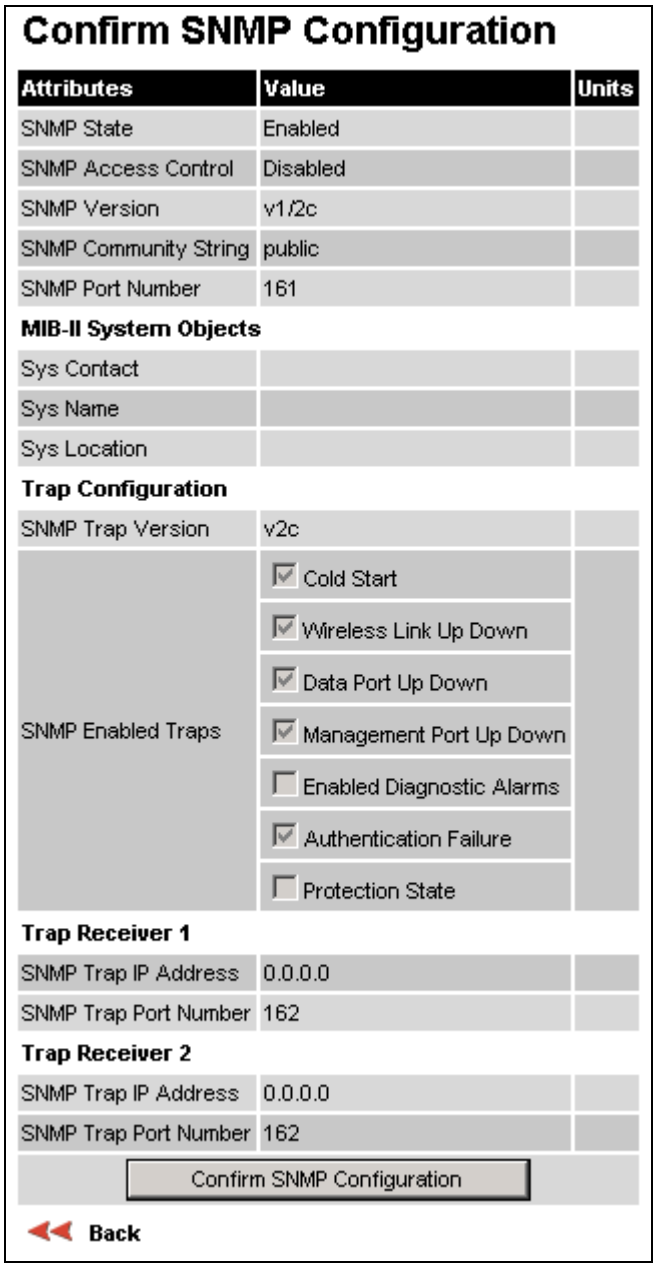
Table 241 Step 3: SNMP Trap Configuration attributes (for SNMPv1/2c)

Attribute	Meaning
SNMP Trap Version	The SNMP protocol version to use for SNMP traps: ‘v1’ or ‘v2c’.
SNMP Enabled Traps	The events that will generate SNMP traps.
SNMP Trap IP Address 1	The IP address of the first SNMP server (trap receiver). This is normally the network management system, but it may be a separate trap receiver. A value of zeros disables logging on the first SNMP server.
SNMP Trap Port Number 1	The server 1 port at which SNMP traps are received.
SNMP Trap IP Address 2	The IP address of the second SNMP server (trap receiver). This is normally the network management system, but it may be a separate trap receiver. A value of zeros disables logging on the second SNMP server.
SNMP Trap Port Number 2	The server 2 port at which SNMP traps are received.

Confirm SNMP Configuration (for SNMPv1/2c)

When the Confirm SNMP Configuration page (Figure 161) is displayed, review the settings and select either **Back** or **Confirm SNMP Configuration and Reboot**. When the settings are confirmed, the unit reboots.

Figure 161 Confirm SNMP Configuration page (for SNMPv1/2c)



Confirm SNMP Configuration

Attributes	Value	Units
SNMP State	Enabled	
SNMP Access Control	Disabled	
SNMP Version	v1/2c	
SNMP Community String	public	
SNMP Port Number	161	
MIB-II System Objects		
Sys Contact		
Sys Name		
Sys Location		
Trap Configuration		
SNMP Trap Version	v2c	
SNMP Enabled Traps	☑ Cold Start	
	☑ Wireless Link Up Down	
	☑ Data Port Up Down	
	☑ Management Port Up Down	
	☐ Enabled Diagnostic Alarms	
	☑ Authentication Failure	
	☐ Protection State	
Trap Receiver 1		
SNMP Trap IP Address	0.0.0.0	
SNMP Trap Port Number	162	
Trap Receiver 2		
SNMP Trap IP Address	0.0.0.0	
SNMP Trap Port Number	162	

Confirm SNMP Configuration

Back

Task 9: Configuring alarms and messages

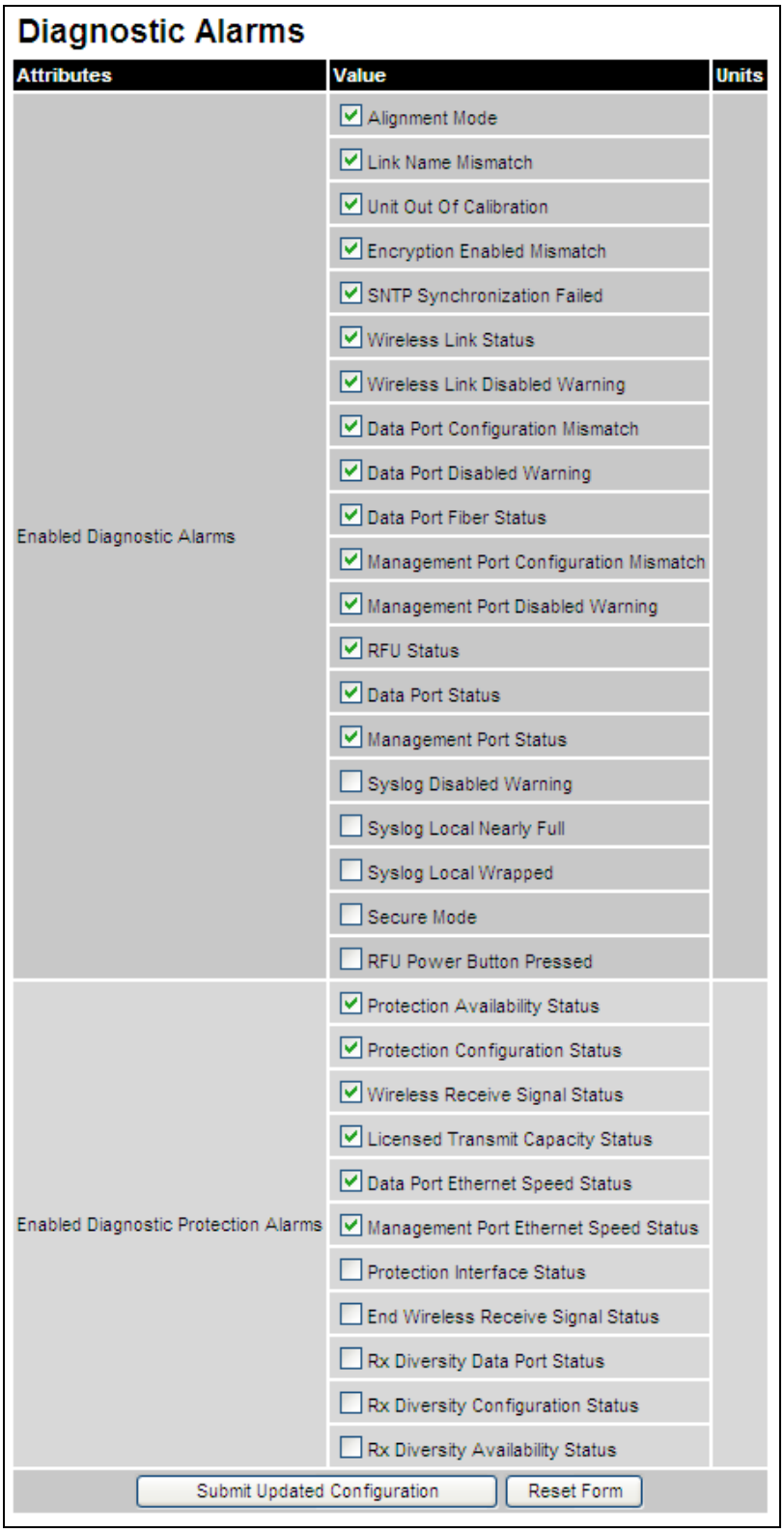
This task consists of the following procedures:

- Configuring generation of diagnostics alarms on page 6-90
- Configuring generation of email messages on page 6-92

Configuring generation of diagnostics alarms

To select which diagnostic alarms will be notified to the system administrator, select menu option **Management, Diagnostic Alarms**. The Diagnostic Alarms page is displayed (Figure 162). These alarms are described in Managing alarms on page 7-15. Tick the boxes against the required alarms, then select **Submit Updated Configuration**.

Figure 162 Diagnostic Alarms page (with protection alarms)



Configuring generation of email messages

To enable the system to generate Simple Mail Transfer Protocol (SMTP) email messages to notify the system administrator when certain events occur, proceed as follows:

1. Select menu option **Management, Email**. The Email Configuration page is displayed (Figure 163).
2. Update the Email Configuration attributes (Table 242).
3. Select **Submit Updated Configuration**. The Configuration Change Reboot dialog is displayed.
4. Select **Reboot Wireless Unit**. The Reboot Confirmation dialog is displayed.
5. Select **OK**. The reboot progress message is displayed. On completion, the unit restarts.

Figure 163 Email Configuration page

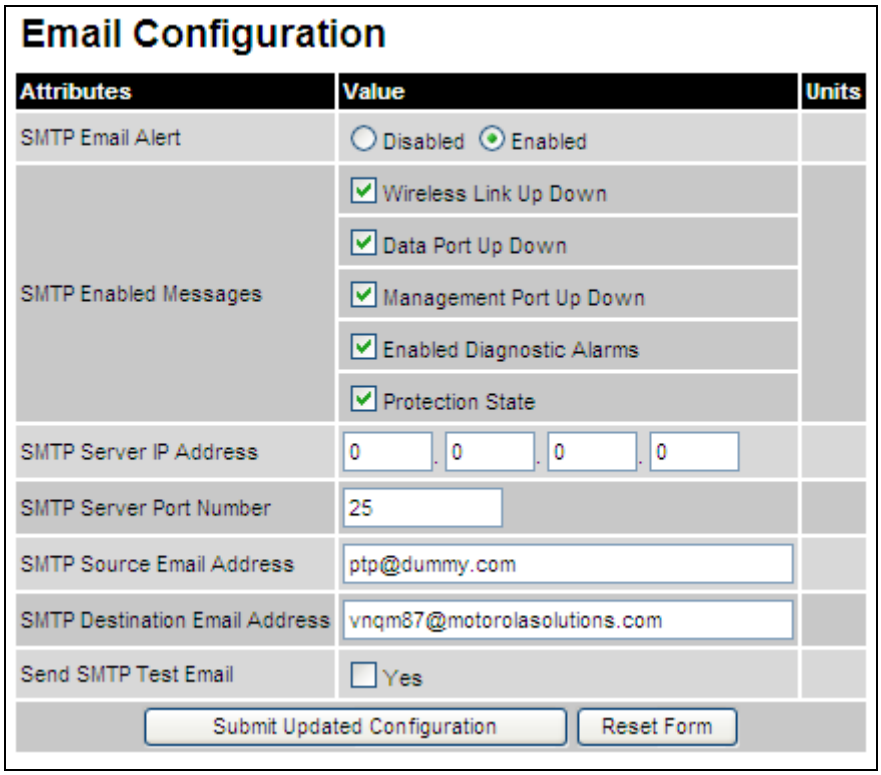


Table 242 Email Configuration attributes

Attribute	Meaning
SMTP Email Alert	Controls the activation of the SMTP client.
SMTP Enabled Messages	The SMTP Enabled Messages attribute controls which email alerts the unit will send.
SMTP Server IP Address	The IP address of the networked SMTP server.
SMTP Server Port Number	The SMTP Port Number is the port number used by the networked SMTP server. By convention the default value for the port number is 25.
SMTP Source Email Address	The email address used by the unit to log into the SMTP server. This must be a valid email address that will be accepted by your SMTP Server.
SMTP Destination Email Address	The email address to which the unit will send the alert messages.
Send SMTP Test Email	Generate and send an email in order to test the SMTP settings. The tick box will self-clear when **Submit** is selected.

Task 10: Configuring syslog

Perform this task when system logging is required.

For more information on syslog, refer to Managing event notification messages on page 7-31.

Configuring system logging (syslog)

Only users with ‘Security Officer’ role are permitted to configure the syslog client.

To configure system logging, select menu option **Management, Syslog, Syslog configuration**. The Syslog Configuration page is displayed (Figure 164). Update the attributes as required (Table 243), then select **Submit Updated Configuration**.

Figure 164 Syslog Configuration page

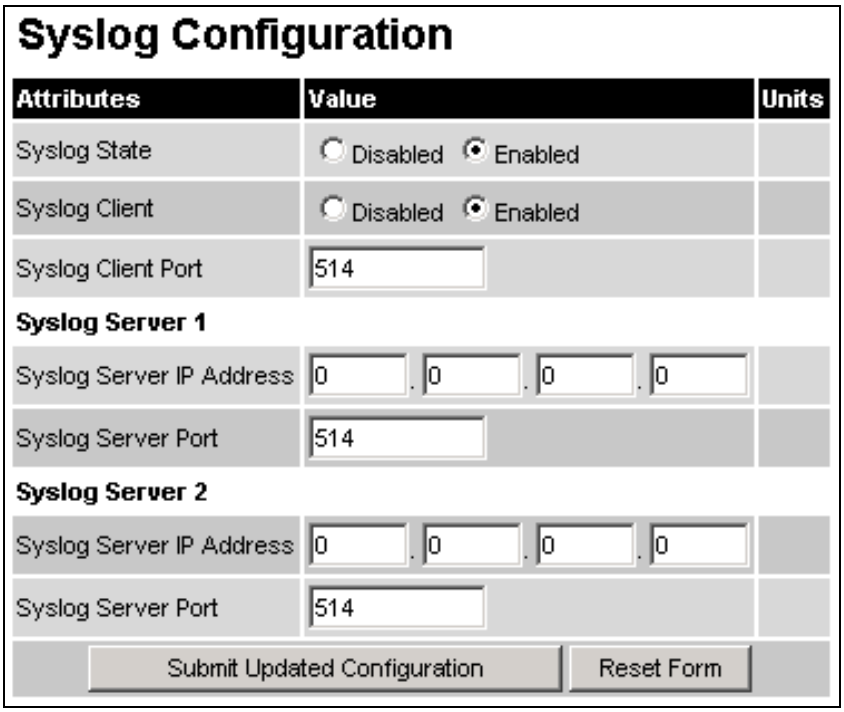


Table 243 Syslog Configuration attributes

Attribute	Meaning
Syslog State	'Enabled' means that system logging is enabled.
Syslog Client	'Enabled' means that the system logging client is enabled.
Syslog Client Port	The client port from which syslog messages are sent.
Syslog Server IP Address 1	The IP address of the first syslog server. A value of zeroes disables logging on the first syslog server.
Syslog Server Port 1	The server 1 port at which syslog messages are received.
Syslog Server IP Address 2	The IP address of the second syslog server. A value of zeroes disables logging on the second syslog server.
Syslog Server Port 2	The server 2 port at which syslog messages are received.

Task 11: Configuring remote access

Configuring web-based management attributes

⚠ CAUTION

If the HTTP, HTTPS, Telnet and SNMP interfaces are all disabled, then it will be necessary to use the Recovery image to reset IP & Ethernet Configuration back to factory defaults to re-enable the interfaces.

NOTE

The HTTP and Telnet interfaces should be disabled if the HTTPS interface is configured. See Configuring HTTPS/TLS page 6-32.

To configure HTTP, Telnet and TFTP access, select menu option **Management, Web**. The Web-Based Management page is displayed (Figure 165). Update the attributes as required (Table 244), then select **Submit Updated Configuration**.

Figure 165 Web-Based Management page

Web-Based Management

Attributes	Value	Units
HTTPS Access Enabled	○ No ◉ Yes	
HTTPS Port Number	443	
HTTP Access Enabled	○ No ◉ Yes	
HTTP Port Number	80	
Telnet Access Enabled	○ No ◉ Yes	
Telnet Port Number	23	
Access Control	◉ Disabled ○ Enabled	
SNMP Control Of HTTP And Telnet	○ Disabled ◉ Enabled	
TFTP Client	○ Disabled ◉ Enabled	
Debug Access Enabled	○ No ◉ Yes	
Cross Site Request Forgery Protection	○ Disabled ◉ Enabled	
Submit Updated Configuration	Reset Form	

Table 244 Web-Based Management attributes

Attribute	Meaning
HTTPS Access Enabled	Only displayed when HTTPS is configured. Shows the current status of HTTPS access (enabled or not).
HTTPS Port Number	Only displayed when HTTPS is configured. The port number for HTTPS access. A value of zero means the wireless unit uses the default port.
HTTP Access Enabled	'No' means that the unit will not respond to any requests on the HTTP port. 'Yes' means that the unit will respond to requests on the HTTP port.
HTTP Port Number	The port number for HTTP access. A value of zero means the wireless unit uses the default port.
Telnet Access Enabled	'No' means that the unit will not respond to any requests on the Telnet port. 'Yes' means that the unit will respond to requests on the Telnet port.
Telnet Port Number	The port number for Telnet access. A value of zero means the wireless unit uses the default port.
Access Control	'Enabled' means that web-based management can be access by IP address. Up to three IP addresses may be entered.
SNMP Control of HTTP And Telnet	'Disabled' means that neither HTTP nor Telnet can be controlled remotely via SNMP. 'Enabled' means that both HTTP and Telnet can be controlled remotely via SNMP.
TFTP Client	'Disabled' means that the unit will not respond to any TFTP software download requests. 'Enabled' means that software can be downloaded via TFTP, as described in Upgrading software on page 7-68.
Debug Access Enabled	'Yes' means that Cambium Technical Support is allowed to access the system to investigate faults.
Cross Site Request Forgery Protection	'Enabled' means that Cross Site Request Forgery Protection is enabled.

Task 12: Aligning antennas

Use the Installation Wizard to set the system into alignment mode, to achieve the lowest possible link loss through correct antenna alignment, and to report on the performance of the configured link.

WARNING

Do not start antenna alignment until it is safe for the antennas to radiate RF, that is, until the antennas and ODUs have been installed on the masts or poles and no personnel are in front of the antennas.

For background on the alignment process, refer to Introduction to antenna alignment on page 6-98.

Check that the requirements in Prerequisites for alignment on page 6-99 have been met.

For a 1+1 Hot Standby link with two antennas at each end of the link, perform Aligning protected antennas on page 6-99.

For an unprotected link, or for a 1+1 Hot Standby link that uses ODU couplers, perform Aligning a pair of antennas on page 6-100.

Introduction to antenna alignment

Licensed microwave links use parabolic dish antennas which have narrow beam widths ranging from 4.7° down to 0.5°. Beam width depends on antenna gain, larger gain antennas having narrower beam widths. It is most important that all PTP 800 antennas are precisely aligned at the centre of the main beam. If antennas are not aligned at the centre of the main beam, performance will be dramatically reduced.

The alignment process requires the elevation angle (vertical plane) and azimuth angle (horizontal plane) to be adjusted. Antenna assemblies provide a mechanism for independently adjusting in both planes whilst the antenna mounting bracket is securely mounted to the mast. Please refer to the instructions provided with the antenna.

Alignment is achieved by monitoring the receive signal strength indicator (RSSI). This is provided at the RFU BNC socket in the form of a dc voltage (RSSI Voltage).

Prerequisites for alignment

Before starting alignment, confirm the following:

- The antennas, cables and CMUs have been installed at both ends of the link.
- A link planning report is available (for example, from LINKPlanner). It should include predicted RSSI voltage ranges (or received signal levels) and bearings for both ends of the link. If the report specifies predicted receive signal levels (dBm) but not voltages, then convert dBm to volts using the formula or graph in RSSI output on page 4-5.
- Two voltmeters with BNC connectors are available.
- No personnel are in front of the antennas.

Aligning protected antennas

For a 1+1 Hot Standby link with two antennas at each end of the link, align each of the following three pairs by following Aligning a pair of antennas on page 6-100:

1. Align the 'Tx Hi' primary antenna to the 'Tx Lo' primary antenna. Do not make any further adjustments to the two primary antennas.
2. Align the 'Tx Hi' secondary antenna to the (now fixed) 'Tx Lo' primary antenna.
3. Align the 'Tx Lo' secondary antenna to the (now fixed) 'Tx Hi' primary antenna.

Step 3 can be performed before step 2, if preferred.

Aligning dual-polar antennas

Perform alignment with either the Horizontal units muted or the Vertical units muted. Take RSSI readings on the unmated units. After alignment, check that the difference in receive power is within tolerance specified in the link planning report.

For more information, refer to the antenna manufacturer's instructions.

Aligning a pair of antennas

Connect the CMUs to a management PC and open the web interfaces at both ends of the link. For more information, see Connecting to the PC and powering up on page 6-6 and Logging into the web interface on page 6-6.

> **NOTE**
> When the **Start Alignment** option is selected, the Installation Wizard automatically enables wireless transmission in alignment mode.

Antennas are aligned by monitoring RFU output voltage and receive power.

Align each pair of antennas by using Step 5, Step 6 and Step 7 of the Installation Wizard, as described in the following procedures:

- Step 5: Starting antenna alignment on page 6-100
- Step 6: Aligning antennas on page 6-100
- Step 7: Completing alignment on page 6-105

Step 5: Starting antenna alignment

At both link ends, check that the Step 5: Start Antenna Alignment page is displayed (Figure 150). If necessary, select menu option **Installation Wizard** and click through Steps 1 to 4 of the wizard.

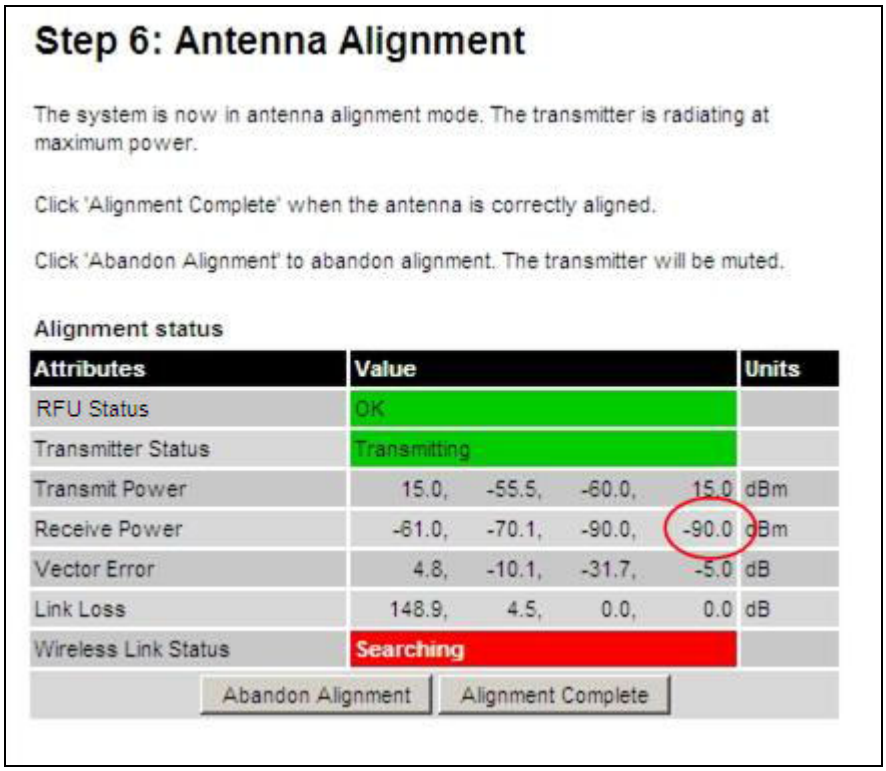
Step 6: Aligning antennas

Select **Start Alignment** at both link ends. The Step 6: Antenna Alignment page is displayed (Figure 166).

> **NOTE**
> In the Step 6: Antenna Alignment page (Figure 166 and Figure 169), Transmit Power, Receive Power, Vector Error and Link Loss are presented as an array of four elements. These elements represent the maximum, mean, minimum and latest values respectively. The maximum, mean and minimum are calculated over a running one hour period.

> **CAUTION**
> During the alignment process, ensure that antenna waveguide and coaxial components are not strained beyond their minimum bend radii.

Figure 166 Step 6: Antenna Alignment page (searching for link)



Preparing for alignment

To prepare the antennas for alignment, proceed as follows at both link ends:

1. Using the instructions provided with the antenna, set the elevation and azimuth adjustment mechanisms to the centre of the range.
2. Using the instructions provided with the antenna, adjust the position of the antenna mounting bracket such that the antenna is pointing at the other end of the link. Use a compass and the bearing provided by the planning report.
3. Once the antenna is in position, resecure the mounting bracket.
4. Connect a suitable voltmeter to the RSSI connector. Figure 8 shows the location of this connector for the ODU and Figure 16 shows the connector on the IRFU. Connect the center of the RSSI connector to the positive terminal of the voltmeter.
5. Use the voltmeter to monitor the RSSI voltage during alignment.

Aligning one end

Align the antenna at one end of the link while keeping the antenna at the other end of the link stationary.

To find the correct elevation and azimuth angles at one end, proceed as follows:

1. Perform a complete sweep of the elevation range of the antenna by adjusting the elevation angle incrementally. The extent of the sweep depends upon antenna gain. Measure RSSI voltage at each point in the sweep.
2. The resulting plot of voltage against elevation should be symmetrical. Record the elevation angle that appears to be at the axis of symmetry, as this is likely to be the correct angle for aligning with the other antenna (Figure 167).

> **NOTE**
> Figure 167 shows the axis of symmetry occurring at a voltage 'peak'. However, it is possible for the axis of symmetry (and therefore the correct elevation angle) to occur at a voltage 'trough' (Figure 168).

3. Set the elevation angle to the axis of symmetry, as identified in the plot.
4. Perform a complete sweep of the azimuth range of the antenna and record the resulting plot of voltage against azimuth.
5. Set azimuth angle to the centre of the range over which the maximum RSSI voltage is recorded.

Figure 167 Symmetrical relationship between voltage and alignment

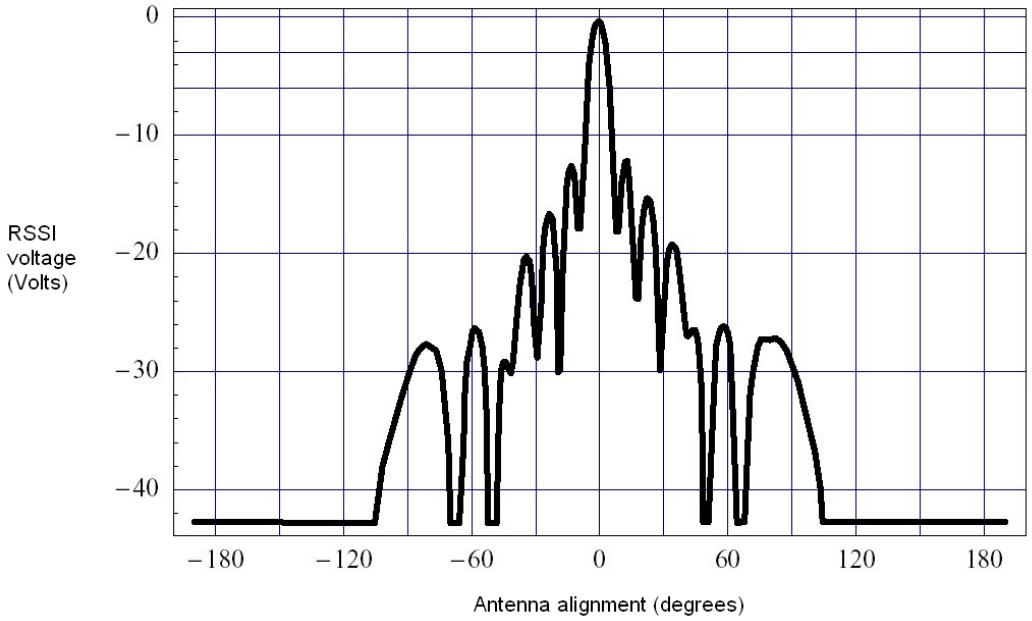
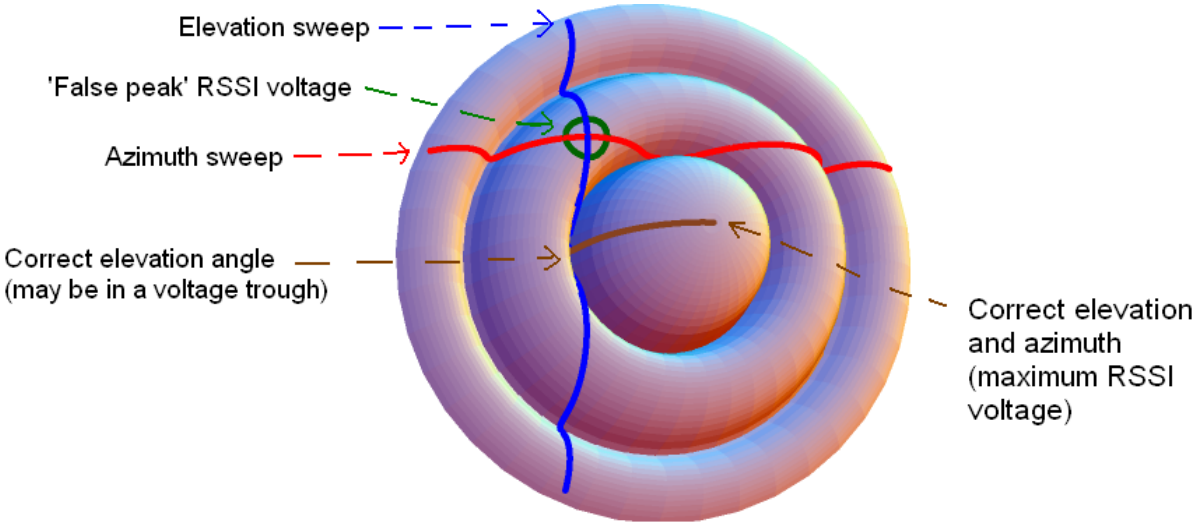


Figure 168 Typical RSSI voltage peaks and troughs



Aligning the other end

Repeat the above procedure at the other end of the link.

Record the RSSI voltage at both ends of the link. If the voltage at either end of the link is not in the range predicted by the planning report, repeat alignment until this is the case.

Post-alignment actions

> **NOTE**
> In a 1+1 Hot Standby link, the tolerances in the ODUs may result in the Receive Power delta between the primary and secondary units at same end of the link being different from the delta predicted by the network designer. Configurations using a single antenna may have up to ±5 dB additional delta when compared with the design value. Where separate antennas are used, the tolerances may increase if either path incurs any Excess Path Loss.

When alignment is complete at both ends, proceed as follows:

1. At each end of the link in turn, lock off and tighten all the adjustment bolts as per the instructions provided with the antenna and check that the RSSI voltage does not change. If it does change, repeat alignment for the affected end.
2. Check that the following requirements are met:

   RSSI voltage at both ends is within the range predicted by the planning report.

   Wireless Link Status is ‘Up’ (green) (Figure 169).

   Receive Power at both end is within the range predicted by the planning report (Figure 169).

3 If any of the above requirements are not met, antenna alignment is not complete; refer to troubleshooting section Installing the link on page 8-9.

4 If all of the above requirements are met, select **Alignment Complete** (Figure 169).

5 If antenna alignment cannot be performed now and must be deferred, select **Abandon Alignment**. This cancels the Install Wizard without doing alignment. The transmitter is muted and the Step 7: Alignment Abandoned page is displayed (Figure 170).

Figure 169 Step 6: Antenna Alignment page (link established)

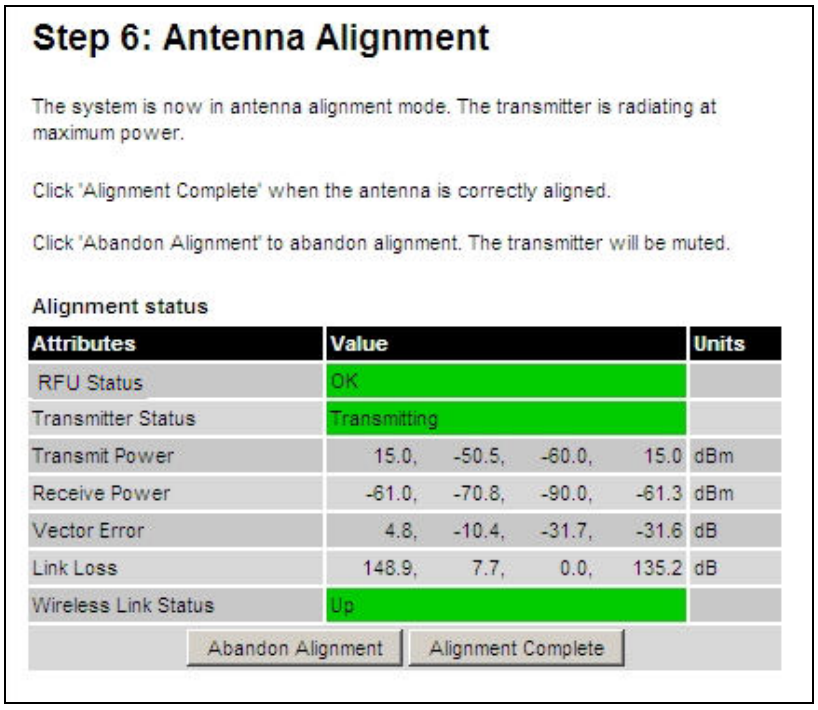
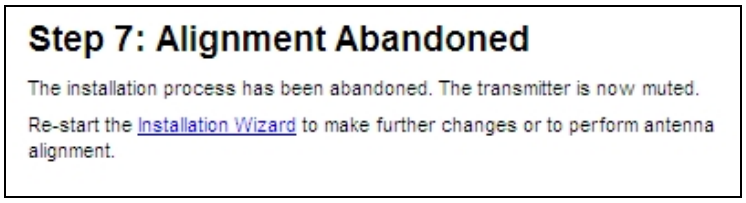


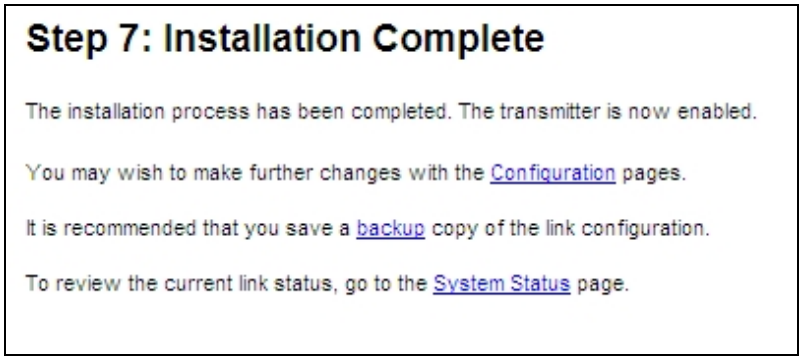
Figure 170 Alignment Abandoned


Step 7: Alignment Abandoned
The installation process has been abandoned. The transmitter is now muted.
Re-start the Installation Wizard to make further changes or to perform antenna alignment.

Step 7: Completing alignment

The Step 7: Installation Complete page is displayed (Figure 171).

Figure 171 Step 7: Installation Complete page


Step 7: Installation Complete
The installation process has been completed. The transmitter is now enabled.
You may wish to make further changes with the Configuration pages.
It is recommended that you save a backup copy of the link configuration.
To review the current link status, go to the System Status page.

Task 13: Reviewing configuration and performance

Perform this task after antenna alignment is complete.

This task consists of the following procedures:

- Reviewing system configuration attributes on page 6-106
- Comparing actual to predicted performance on page 6-110

Reviewing system configuration attributes

To review and update the system configuration of a PTP 800 link, select menu option **System, Configuration**. The Installation Configuration page is displayed (Figure 172). Review the attributes (Table 245), update them as required, and select **Submit Updated System Configuration**:

If any other attributes are incorrect, update them by following the procedures in this chapter.

Figure 172 Installation Configuration page

Installation Configuration

This page primarily displays the configuration entered during installation of the link. Some configuration attributes may be modified on this page. To modify other attributes displayed on this page, please select Installation.

Attributes	Value	Units
Transmitter	Enabled	
	Mute Transmitter	

Attributes	Value	Units
Link		
Link Name	Rack RBW4	
Site Name	Site1	
Antenna		
Antenna Gain	0.0	dBi
RF Feeder Loss	0.0	dB
IF Cable		
IF Cable Length	0	m
Modem		
Short Power Cycle For Recovery	Disabled	
RFU		
RFU Receive Branching Unit Loss	0.0	dB
RFU Transmit Branching Unit Loss	0.0	dB
Radio License		
Radio License Identifier		
Radio License Band	Lower 6 GHz	
Radio License Region	FCC	
Radio License Bandwidth	30 MHz	
Radio License Max EIRP	100.0	dBm
Radio License Tx Freq	6226.890	MHz
Radio License Rx Freq	5974.850	MHz
Radio License Modulation Selection	Fixed Modulation	
Radio License Mod Mode	256QAM 0.80	
Wireless		
Maximum Transmit Power (Max 22.0, Min 9.0)	22.0	dBm
EIRP	22.0	dBm
Encryption Algorithm	None / AES 128-bit (Rijndael) / AES 256-bit (Rijndael)	
Encryption Key		
Confirm Encryption Key		
Automatic Transmitter Power Control	Disabled / Enabled	
	Submit Updated System Configuration / Reset Form	

Table 245 System Configuration attributes

Attribute	Meaning
Transmitter	'Muted' means that the RFU will not radiate and the CMU will not forward Ethernet Frames between the wireless interface and the Ethernet ports. This applies in all conditions. 'Enabled' means that the RFU is allowed to radiate and the CMU is allowed to forward Ethernet Frames between the wireless interface and the Ethernet Ports. However, other factors may still prevent this, for example if the unit is the inactive unit at an end of a 1+1 Hot Standby link. To change the state from 'Muted' to 'Enabled', select **Enable Transmitter**. To change the state from 'Enabled' to 'Muted', select **Mute Transmitter**. NOTE This attribute does not indicate whether the unit is actually radiating and forwarding Ethernet Frames but is a configuration attribute allowing the unit to radiate and forward traffic if other factors permit. To see if the unit is actually radiating and forwarding traffic, examine the Transmitter Status attribute, which is available on the Status page.
Link	
Link Name	Read only. This attribute is set in the Installation wizard (Table 232).
Site Name	The Site Name can be updated.
Antenna	
Antenna Gain	Read only. This attribute is set in the Installation wizard (Table 232).
RF Feeder Loss	Read only. This attribute is set in the Installation wizard (Table 232).
IF Cable	
IF Cable Length	Read only. This attribute is set in the Installation wizard (Table 232).
Modem	

Attribute	Meaning
Short Power Cycle for Recovery	Read only. This attribute is set in the Installation wizard (Table 232).
Radio License	
	These attributes are read only, as they are set in the Installation wizard (Table 233).
Wireless	
Maximum Transmit Power	The maximum transmit power that the local wireless unit is permitted to use to sustain a link.
EIRP	The actual EIRP in dBm.
Max Mod Mode	The maximum modulation mode the radio can use when ACM is enabled. The valid range is dependant on the region, license and Tx Max Power. This control is only visible for certain regions when Radio License Modulation Selection is set to 'Adaptive'.
Min Mod Mode	The minimum modulation mode the radio can use when ACM is enabled. The valid range is dependant on the region, license and Tx Max Power. This control is only visible for certain regions when Radio License Modulation Selection is set to 'Adaptive'.
Encryption Algorithm	This is set in Configuring AES encryption on page 6-29.
Encryption Key	This is set in Configuring AES encryption on page 6-29.
Automatic Transmitter Power Control	Enable or disable ATPC. In regions and bands where ATPC is a regulatory requirement, for example 18 GHz Europe, this cannot be disabled.

Comparing actual to predicted performance

For at least one hour of operation after alignment is complete, monitor the link should to check that it is achieving predicted levels of performance.

To check performance, select menu option **System, Statistics**. The System Statistics and Counters page is displayed (Figure 194). Monitor the following attributes:

- Link Loss
- Transmit Data Rate
- Receive Data Rate
- Receive Power: To maintain error free communication, ensure that the average operational Receive Power, using ATPC if enabled, does not exceed -35 dBm. If Receive Power exceeds -35 dBm, enable ATPC if currently disabled. Alternatively, reduce the Maximum Transmit Power at the other end of the link to reduce the Receive Power at this end. If the Receive Power still exceeds -35 dBm, install a fixed waveguide attenuator (this requires a remote mount antenna).

PTP LINKPlanner provides the prediction in the form of an installation report.

NOTE

In a 1+1 Hot Standby link, the tolerances in the ODUs may result in the Receive Power delta between the primary and secondary units at same end of the link being different from the delta predicted by the network designer. Configurations using a single antenna may have up to ±5 dB additional delta when compared with the design value. Where separate antennas are used, the tolerances may increase if either path incurs any Excess Path Loss.

For more information, refer to Checking system statistics and counters on page 7-57.

Task 14: Configuring quality of service

Configuring quality of service

To configure the classification of priority encoded Ethernet frames into up to eight traffic classes, select menu option **System**, **Configuration, QoS Configuration**. The QoS Configuration page is displayed (Figure 173 or Figure 174).

Update the Layer 2 Control Protocols (Table 246) and Ethernet Priority Queue mapping (Table 247) as required.

To use IEEE 802.1Q classification rules, select **Reset Default Priority Mappings**. The 802.1Q rules are shown in Table 247.

Select **Submit Updated Configuration**.

Figure 173 QoS Configuration page (Ethernet)

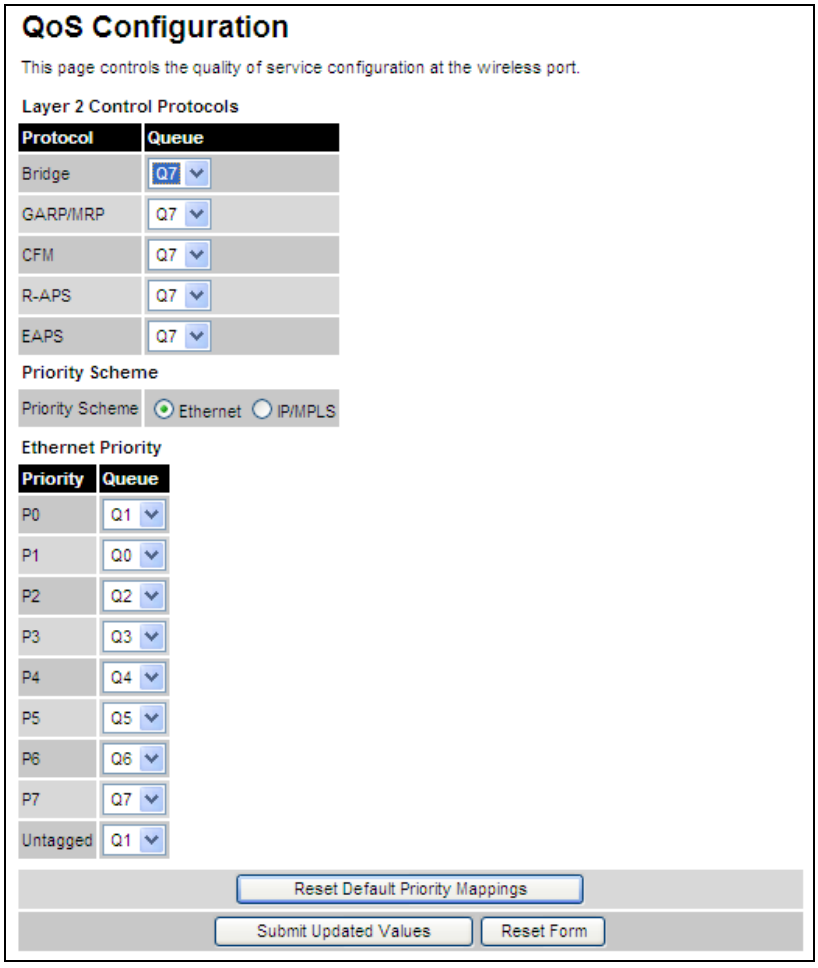


Figure 174 QoS Configuration page (IP/MPLS)



Table 246 Layer 2 Control Protocols

Attribute	Meaning
Bridge	The classification of each layer 2 control protocol (L2CP) to an egress queue at the wireless port.
MRP	
CFM	
R-APS	
EAPS	
Priority Scheme	Classification is based on fields in the Ethernet header (Layer 2) or in the Network header (Layer 3). The unit recognizes two network layer protocols: IP and MPLS.
Unknown Protocol	The classification of unknown network protocols (not IP or MPLS) to an egress queue at the wireless port. Only displayed when Priority Scheme is IP/MPLS.

Table 247 Ethernet Priority Queue settings

VLAN Priority	IEEE802.1Q traffic class
P0	Q1
P1	Q0
P2	Q2
P3	Q3
P4	Q4
P5	Q5
P6	Q6
P7	Q7
Untagged	Q1

Task 15: Connecting link to the network

Perform this task to connect to the network and set the system clock.

This task consists of the following procedures:

- Connecting to the network on page 6-114
- Setting the real-time clock on page 6-115
- Saving the system configuration on page 6-119

Connecting to the network

To complete and test the network connections, proceed as follows:

1. Disconnect the local PC from the CMU management port at each CMU.
2. Connect the CMUs to the network equipment using the cables that were prepared in Preparing network connections (1+0 and 2+0 links) on page 5-84 or Preparing network connections (1+1 Hot Standby) on page 5-89.
3. Check that each of the CMUs is reachable from the network management system by opening the web interface to the management agents, or by requesting ICMP echo response packets using the Ping application. The network management system will normally be geographically remote from the site, so it may be necessary to request that this action is completed by co-workers at the management centre. Alternatively, it may be possible to use remote login to the management system.

   NOTE
   For testing the remote end of a link with in-band management, the wireless link may need to be operational first.

4. Check that the data network operates correctly across the wireless link. This may be by requesting ICMP echo response packets between hosts in the connected network segments, or by some more structured use of network testing tools.
5. For a 1+1 Hot Standby link:

   Initiate a protection switch at one end of the link (as described in Forcing protection switches on page 7-37) and check that the data network operates correctly across the wireless link (as described in the previous step).

   Initiate a switch back to the primary unit.

   Repeat for the other end of the link.

6 For a 1+1 Hot Standby link, re-enable automatic fault protection switching by setting the Fault Protection Switching attribute to 'Enabled', as described in Configuring 1+1 Hot Standby links on page 6-54.

Repeat for the other end of the link.

7 Check that the wireless interface is enabled at both ends, as described in Enabling wireless transmission on page 7-32.

For a 1+1 Hot Standby link, check that both units are enabled at each end.

8 Select menu option **Home** and check that there are no alarms on any unit. For more information, see Managing alarms on page 7-15.

Setting the real-time clock

The clock supplies accurate date and time information to the CMU. It can be set to run with or without a connection to a network time server (SNTP):

- In the absence of an SNTP server connection, set the clock to run manually. The clock is battery backed and will continue to operate for several days after the CMU is switched off.
- If an SNTP server connection is available, set the clock to synchronize with the server time at regular intervals.

Setting the real-time clock manually

To set the CMU clock to keep time without connecting to a networked time server, select menu option **Management, Time**. The Time Configuration page is displayed. Set the SNTP State attribute to 'Disabled': the manual clock attributes are displayed (Figure 175). Review and update the manual clock attributes (Table 248), then select **Submit Updated Configuration**.

Figure 175 Time Configuration page (SNTP disabled)

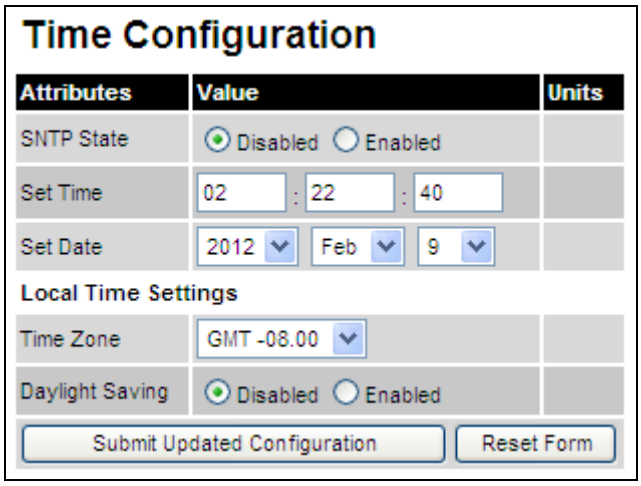


Table 248 Manual clock attributes

Attribute	Meaning
SNTP State	'Disabled' means that the CMU will keep time without connecting to a networked time server.
Set Time	Current time in hours, minutes and seconds.
Set Date	Current year, month and day.
Time Zone	The time zone offset from Greenwich Mean Time (GMT).
Daylight Saving	'Disabled' means that daylight saving adjustments will not be applied to the time. 'Enabled' means that daylight saving adjustments will be applied to the time, according to local rules.

Setting the real-time clock to synchronize using SNTP

To set the clock to synchronize with a networked time server, select menu option **Management, Time**. The Time Configuration page is displayed. Set the SNTP State attribute to 'Enabled': the SNTP clock attributes are displayed (Figure 176). Review and update the SNTP clock attributes (Table 249), then select **Submit Updated Configuration**.

Figure 176 Time Configuration page (SNTP enabled)

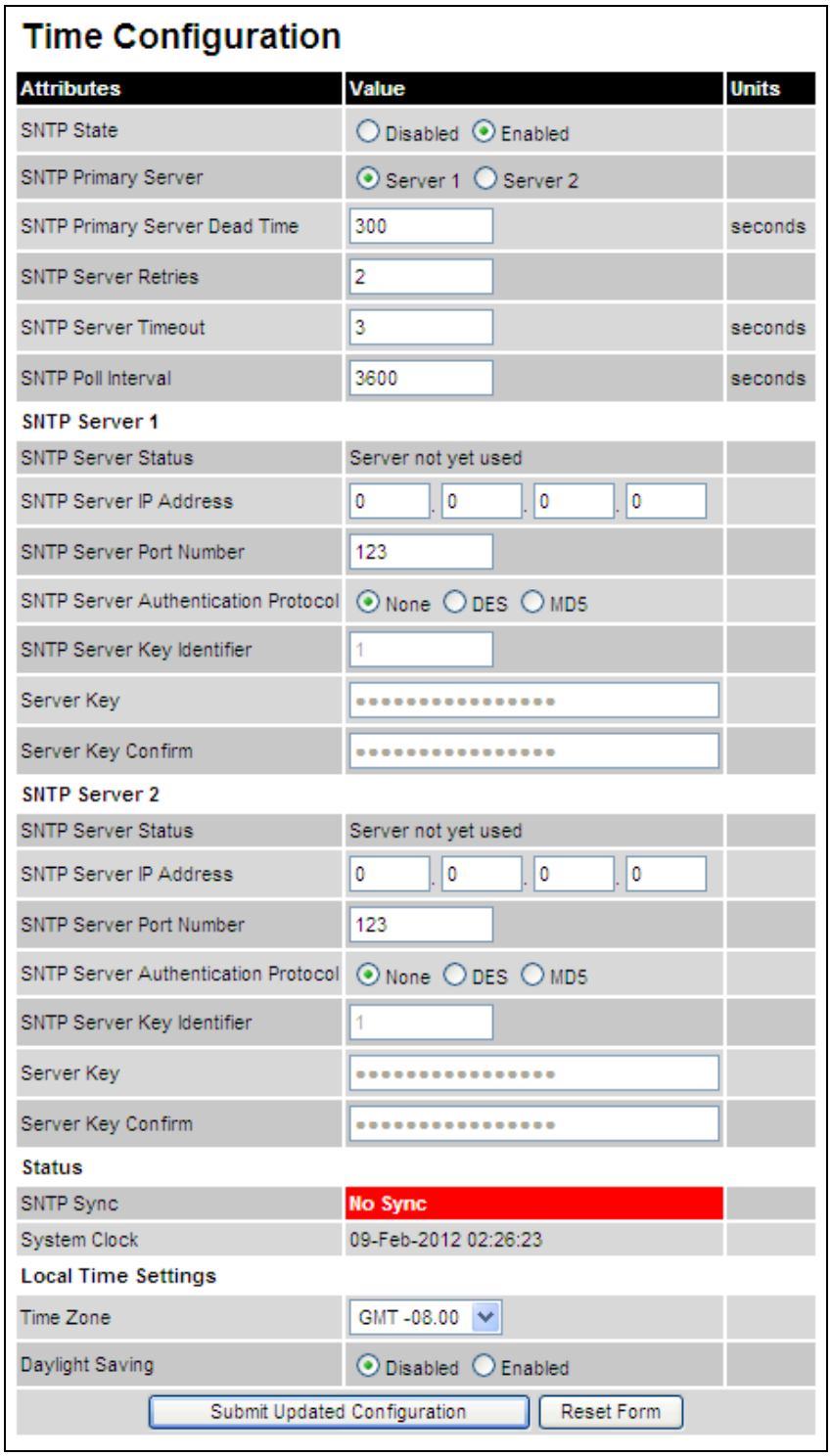


Table 249 SNTP clock attributes

Attribute	Meaning
SNTP State	'Enabled' means that the CMU will obtain accurate date and time updates from a networked time server.
SNTP Primary Server	Specifies the primary SNTP server, determining the order in which the servers are tried.
SNTP Primary Server Dead Time	Time (in seconds) to wait before retrying communications with an unresponsive primary SNTP server. A value of zero disables the timer.
SNTP Server Retries	Number of times the PTP will retry after an SNTP server fails to respond.
SNTP Server Timeout	Time (in seconds) the PTP will wait for a response from an SNTP server.
SNTP Poll Interval	The period at which the SNTP client polls the server for time correction updates (default 1 hour). If an SNTP poll fails, the client will automatically perform three retries before waiting for the user defined poll period.
SNTP Server 1 and 2:	
SNTP Server Status	Status message reflecting the state of communications with the SNTP server.
SNTP Server IP Address	The IP address of the networked SNTP server.
SNTP Server Port Number	The port number of the networked SNTP server. By convention the default value for the port number is 123.
SNTP Server Authentication Protocol	Authentication protocol to be used with this SNTP server (None, DES or MD5).
SNTP Server Key Identifier	SNTP key identifier. A key of zeros is reserved for testing.
Server Key	Key used to authenticate SNTP communications. For DES keys this must be 16 hexadecimal characters as per the DES specification, with the least significant bit of each pair used to maintain odd parity.
Server Key Confirm	Must match the server key.
Status:	

Attribute	Meaning
SNTP Sync	The current status of SNTP synchronization. A change of state may generate an SNMP trap or SMTP email alert. **NOTE** If 'No Sync' is displayed, then review the SNTP Server IP Address and Port Number.
SNTP Last Sync	The date and time of the last SNTP synchronization.
System Clock	The local time, allowing for the Time Zone and Daylight Saving settings.
Local Time Settings:	
Time Zone	The time zone offset from Greenwich Mean Time (GMT). 'GMT 00.00' means that the clock is set to UTC time.
Daylight Saving	'Disabled' means that daylight saving adjustments will not be applied to the time. This option is required for UTC time. 'Enabled' means that daylight saving adjustments will be applied to the time, according to local rules.

Saving the system configuration

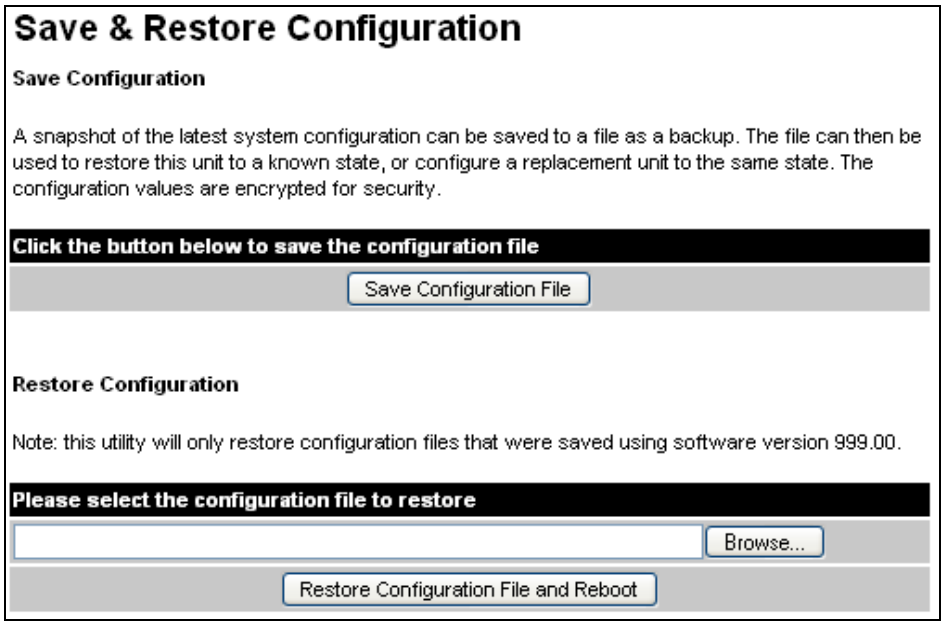
Save the system configuration in the following situations:

- After a new unit has been fully configured as described in this chapter.
- After any change has been made to the configuration.
- Before upgrading the unit to a new software version.
- After upgrading the unit to a new software version.

NOTE
The process for restoring a PTP 800 CMU to a previously saved configuration is described in Restoring the system configuration on page 7-67.

To save the current configuration, select menu option **System, Configuration, Save And Restore**. The Save & Restore Configuration page is displayed (Figure 177). Select **Save Configuration File**. Save the configuration file to a PC hard drive.

Figure 177 Save & Restore Configuration page


Save & Restore Configuration
Save Configuration
A snapshot of the latest system configuration can be saved to a file as a backup. The file can then be used to restore this unit to a known state, or configure a replacement unit to the same state. The configuration values are encrypted for security.
Click the button below to save the configuration file
Save Configuration File
Restore Configuration
Note: this utility will only restore configuration files that were saved using software version 999.00.
Please select the configuration file to restore
Browse...
Restore Configuration File and Reboot

The configuration file format is:

MAC-mm-mm-mm_IP-iii-iii-iii-iii.cfg

Where:	**Is:**
mm-mm-mm	MAC address of unit
iii-iii-iii-iii	IP address of unit.

Configuring for FIPS 140-2 applications

Perform these procedure to allow the unit to operate in FIPS 140-2 secure mode. For more information, refer to FIPS 140-2 on page 1-70 and Planning for FIPS 140-2 operation on page 2-24.

Prerequisites for FIPS 140-2 configuration

To confirm that all prerequisites for FIPS 140-2 are ready, proceed as follows:

1. Ensure that the following cryptographic material has been generated using a FIPS-approved cryptographic generator:

   Key Of Keys

   TLS Private Key and Public Certificates (for the correct IP address)

   Entropy Input

   Wireless Link Encryption Key for AES

2. Ensure that the CMU tamper evident labels have not be interfered with (Figure 36).
3. Identify the Port number for HTTPS.
4. Ensure that the web browsers used are enabled for HTTPS/TLS operation using FIPS-approved cipher specifications.
5. Select menu option **Management, Web, Local User Accounts** and check that the current user's role is Security Officer.
6. Perform Task 3: Installing license keys on page 6-21 and ensure that the installed license key meets all requirements including FIPS 140-2 compatibility:

   Check that Security Level is ‘FIPS’.

   Check that Encryption Algorithm is ‘AES….’.

   If necessary, generate and enter a new license key with the above settings.
7. Perform Task 4: Upgrading software version on page 6-25 and ensure that the installed software version is prefixed `FIPS-`. If necessary, upgrade to the latest FIPS validated image.

8 To confirm that the above steps have been completed, check that the ‘FIPS 140-2 Validated’ logo is displayed in the Navigation Bar:



Configuration procedures for FIPS 140-2

To activate FIPS 140-2 secure mode, perform the following procedures:

- Using the Security Wizard on page 6-33.
- Configuring local user accounts on page 6-42, taking care to complete the following additional settings:
  - Select **Set Best Practice Complexity**.
  - Configure appropriate identity-based user names and passwords.

Checking that the unit is in FIPS 140-2 secure mode

To confirm that the unit is now in FIPS 140-2 secure mode, select menu option **Home** and look for the FIPS Operational Mode Alarm:

- If the FIPS Operational Mode Alarm is NOT present, the unit is in FIPS 140-2 mode.
- If the alarm is present and has the value ‘FIPS mode is not configured’, return to Using the Security Wizard on page 6-33 and check that all Security Wizard settings are correct for FIPS 140-2.
- If the alarm is present and has the value ‘FIPS mode is configured, but not active’, return to Step 7: HTTP and Telnet settings on page 6-39 and check the following attributes:

  HTTP Access Enabled: should be ‘No’.

  Telnet Access Enabled: should be ‘No’.

  SNMP Control of HTTP And Telnet: should be ‘Disabled’.

NOTE

If it is necessary to exit from FIPS 140-2 mode, refer to Exiting FIPS 140-2 mode on page 7-51.

HTTPS key size warning

If the HTTPS key size warning alarm (Figure 178) is present in the Home page, no immediate action is necessary, as this alarm does not block the transition to FIPS 140-2 secure mode. This alarm is produced because FIPS 140-2 recommends a TLS Private Key of at least 2048 bits, but a 1024 bit key has been entered. To clear this alarm, generate a new TLS certificate with key length of at least 2048 bits, then return to Step 2: TLS private key and public certificate on page 6-35.

Figure 178 HTTPS key size warning alarm



Chapter 7: Operation

This chapter describes how to operate a PTP 800 link.

The following topics are described in this chapter:

- Web-based management on page 7-2 describes the layout and the main menu options of the PTP 800 web-based management interface.
- Managing alarms and events on page 7-15 describes how to manage PTP 800 system alarms and events.
- Disabling and enabling the wireless interface on page 7-32 describes how to disable wireless transmission (prevent antenna radiation) and enable wireless transmission (allow antenna radiation).
- Managing 1+1 Hot Standby links on page 7-33 describes how to manage 1+1 links, and how to force protection switches and inhibit protection switching.
- Managing security on page 7-51 describes how to manage security features such as FIPS 140-2 mode and AES encryption in operational PTP 800 links.
- Managing performance on page 7-57 describes how to view and manage PTP 800 system statistics and diagnostics.
- Restoring, upgrading and rebooting on page 7-67 describes how to restore the system configuration, upgrade the software and reboot the unit.
- Using recovery mode on page 7-71 describes how the CMU enters recovery mode and how to recover the CMU.

Web-based management

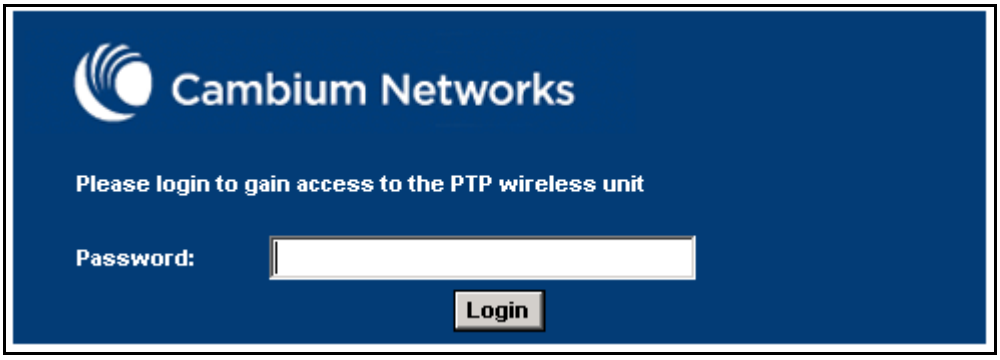
This section describes the layout and the main menu options of the PTP 800 web-based management interface.

Accessing the web interface

The web interface is best viewed using a screen resolution of at least 1024 x 768 pixels. The web pages have been tested with Internet Explorer 7, Internet Explorer 8, Firefox 3 and Firefox 3.5. Other browsers have not been tested.

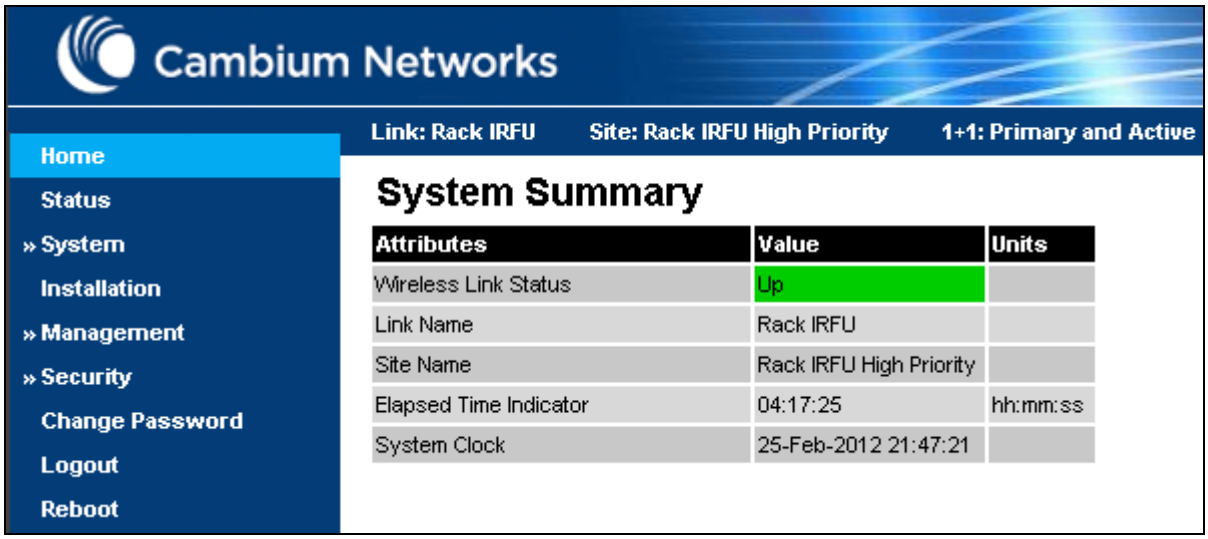
To access the web interface, type the IP address of the unit into the browser address bar and press ENTER. If the Login page (Figure 179) is displayed, enter Password (if set) and select **Login**.

Figure 179 System Administration Login page



The web interface consists of the title bar at the top, the menu bar on the left, and the web page (for the selected menu option) on the right (Figure 180).

Figure 180 Menu and System Summary page (wireless link up)



CAUTION

To maintain security, users must log out of the web interface at the end of a session.

CAUTION

The System Administration menu options are not password protected until a password has been set. For more information, see Protecting access to the summary and status pages on page 6-49.

NOTE

If there is no user activity for a set period of time, the system administrator is automatically logged off. To change the automatic logout time period, or to disable automatic logout, see Changing the log-out timer on page 7-56.

Using the menu options

All web pages contain the menu navigation bar on the left hand side. The menu is used to navigate to other web pages. The currently selected option is always highlighted with a light blue background.

Table 250 lists the procedures that may be performed from each menu option. Many of these procedures are part of the initial configuration and alignment process described in Chapter 6: Configuration and alignment.

Table 250 Procedures performed from each menu option

Menu option	Procedures
Home	Viewing the system summary on page 7-6
Status	Viewing the system status on page 7-7 Checking the installed software version on page 6-25
« System	
« Configuration	Configuring AES encryption on page 6-29 Reviewing system configuration attributes on page 6-106 Disabling wireless transmission on page 7-32 Enabling wireless transmission on page 7-32 Disabling AES encryption on page 7-52 Changing AES encryption keys on page 7-53
LAN Configuration	Configuring the IP interface and management mode on page 6-10
SFP Configuration	This option is only available when an SFP module is fitted. It displays information about the SFP module. There is no associated procedure.
QoS Configuration	Configuring quality of service on page 6-111
Save And Restore	Saving the system configuration on page 6-119 Restoring the system configuration on page 7-67
Protection	Task 6: Configuring protection on page 6-53
Protected Link	Managing 1+1 Hot Standby links on page 7-33 This menu option is only available if 1+1 protection has been configured; see Configuring 1+1 Hot Standby links on page 6-54.

Menu option	Procedures
« Statistics	Comparing actual to predicted performance on page 6-110 Checking system statistics and counters on page 7-57 Resetting system statistics and counters on page 7-62
Detailed Counters	
« Diagnostics	Viewing diagnostics on page 7-62
Diagnostics Plotter	Using the diagnostics plotter on page 7-63 Changing the diagnostics refresh period on page 7-65
CSV Download	Downloading diagnostic data on page 7-64
License Key	Checking licensed capabilities on page 6-21 Entering a new license key on page 6-23
Software Upgrade	Upgrading to a new software version on page 6-26
Installation	Task 7: Configuring wireless interface on page 6-63 Task 12: Aligning antennas on page 6-98
« Management	
« Web	Configuring web-based management attributes on page 6-96
Local User Accounts	Configuring local user accounts on page 6-42 Setting password complexity on page 6-45 Creating or updating identity-based users on page 6-47
RADIUS Configuration	Configuring RADIUS authentication on page 6-50
Login Information	Displaying login information on page 7-52
Web Properties	Protecting access to the summary and status pages on page 6-49 Identifying a unit from the web browser title on page 7-12
SNMP	Configuring SNMPv3 agent on page 6-77 Configuring SNMPv1/2c agent on page 6-86
Email	Configuring generation of email messages on page 6-92
Diagnostic Alarms	Configuring generation of diagnostics alarms on page 6-90
Time	Setting the real-time clock on page 6-115
« Syslog	Managing event notification messages on page 7-31
Syslog Configuration	Configuring system logging (syslog) on page 6-94
« Security	Configuring HTTPS/TLS on page 6-32

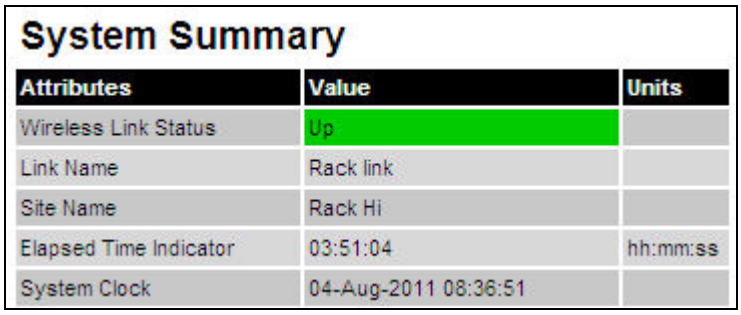
Menu option	Procedures
Zeroize CSPs	Zeroizing critical security parameters on page 7-51
Change Password	Changing own user password on page 6-48
Logout	Logging out on page 7-14
Reboot	Rebooting on page 7-69

Viewing the system summary

To display the System Summary page, select menu option **Home**.

The System Summary page (Figure 181) contains a high level summary of the status of the wireless link and associated equipment.

Figure 181 System Summary page



The System Summary page displays any uncleared system alarms below the System Clock attribute. Whenever system alarms are outstanding, a yellow warning triangle is displayed on the navigation bar. For more information, refer to Managing alarms on page 7-15.

NOTE

Password protection can be extended to cover the System Summary page. For more information, see Protecting access to the summary and status pages on page 6-49.

The attributes of the System Summary page are described in Table 251.

Table 251 System Summary attributes

Attribute	Meaning
Wireless Link Status	Current status of the wireless link. A green background with status text ‘Up’ means that the point-to-point link is established. A red background with suitable status text (for example ‘Searching’) indicates that the link is not established.

Attribute	Meaning
Link Name	The name of the PTP link, as set in the Installation wizard. The Link Name must be the same at both sites, as it is used to establish a connection with the other site.
Site Name	The name given to the site by the system administrator and set by the Installation wizard.
Elapsed Time Indicator	The time (hh:mm:ss) that has elapsed since the last system reboot. The system can reboot for several reasons, for example, commanded reboot from the system reboot webpage, or a power cycle of the equipment.
System Clock	The CMU clock presented as local time, allowing for zone and daylight saving.
Status attributes	Status attributes may be displayed in the System Summary page to indicate abnormal states.

Viewing the system status

To display the System Status page, select menu option **Status**.

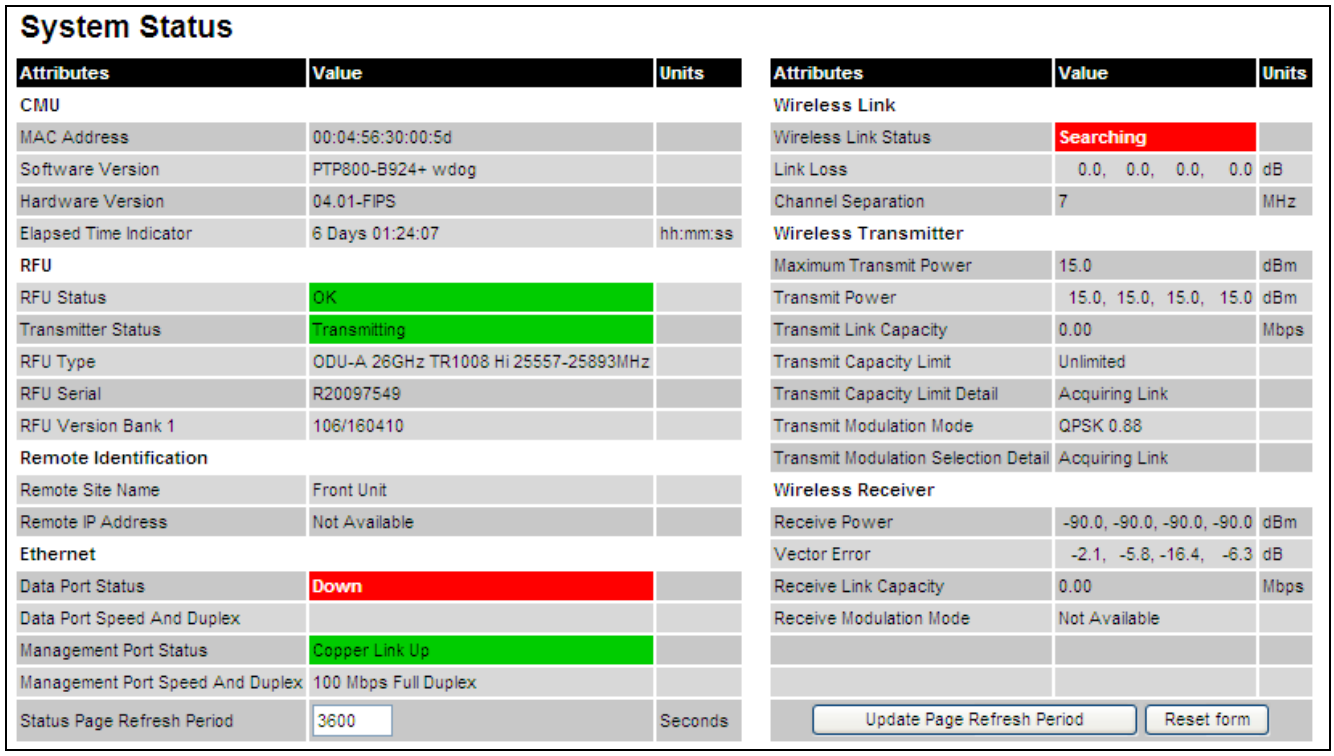
The System Status page (Figure 182) gives the user a detailed view of the operation of the PTP 800 from both the wireless and network perspectives.

The contents of the System Status page depend upon the configuration of the PTP 800. For example, for in-band management of an unprotected unit, no status information is shown for the unused Management Port. For an unprotected link, no status information is shown relating to protection.

NOTE

Password protection can be extended to cover the System Status page. For more information, see Protecting access to the summary and status pages on page 6-49.

Figure 182 System Status page (unprotected link)



System Status

Attributes	Value	Units
CMU		
MAC Address	00:04:56:30:00:5d	
Software Version	PTP800-B924+ wdog	
Hardware Version	04.01-FIPS	
Elapsed Time Indicator	6 Days 01:24:07	hh:mm:ss
RFU		
RFU Status	OK	
Transmitter Status	Transmitting	
RFU Type	ODU-A 26GHz TR1008 Hi 25557-25893MHz	
RFU Serial	R20097549	
RFU Version Bank 1	106/160410	
Remote Identification		
Remote Site Name	Front Unit	
Remote IP Address	Not Available	
Ethernet		
Data Port Status	Down	
Data Port Speed And Duplex		
Management Port Status	Copper Link Up	
Management Port Speed And Duplex	100 Mbps Full Duplex	
Status Page Refresh Period	3600	Seconds

Attributes	Value	Units
Wireless Link		
Wireless Link Status	Searching	
Link Loss	0.0, 0.0, 0.0, 0.0	dB
Channel Separation	7	MHz
Wireless Transmitter		
Maximum Transmit Power	15.0	dBm
Transmit Power	15.0, 15.0, 15.0, 15.0	dBm
Transmit Link Capacity	0.00	Mbps
Transmit Capacity Limit	Unlimited	
Transmit Capacity Limit Detail	Acquiring Link	
Transmit Modulation Mode	QPSK 0.88	
Transmit Modulation Selection Detail	Acquiring Link	
Wireless Receiver		
Receive Power	-90.0, -90.0, -90.0, -90.0	dBm
Vector Error	-2.1, -5.8, -16.4, -6.3	dB
Receive Link Capacity	0.00	Mbps
Receive Modulation Mode	Not Available	

Update Page Refresh Period | Reset form

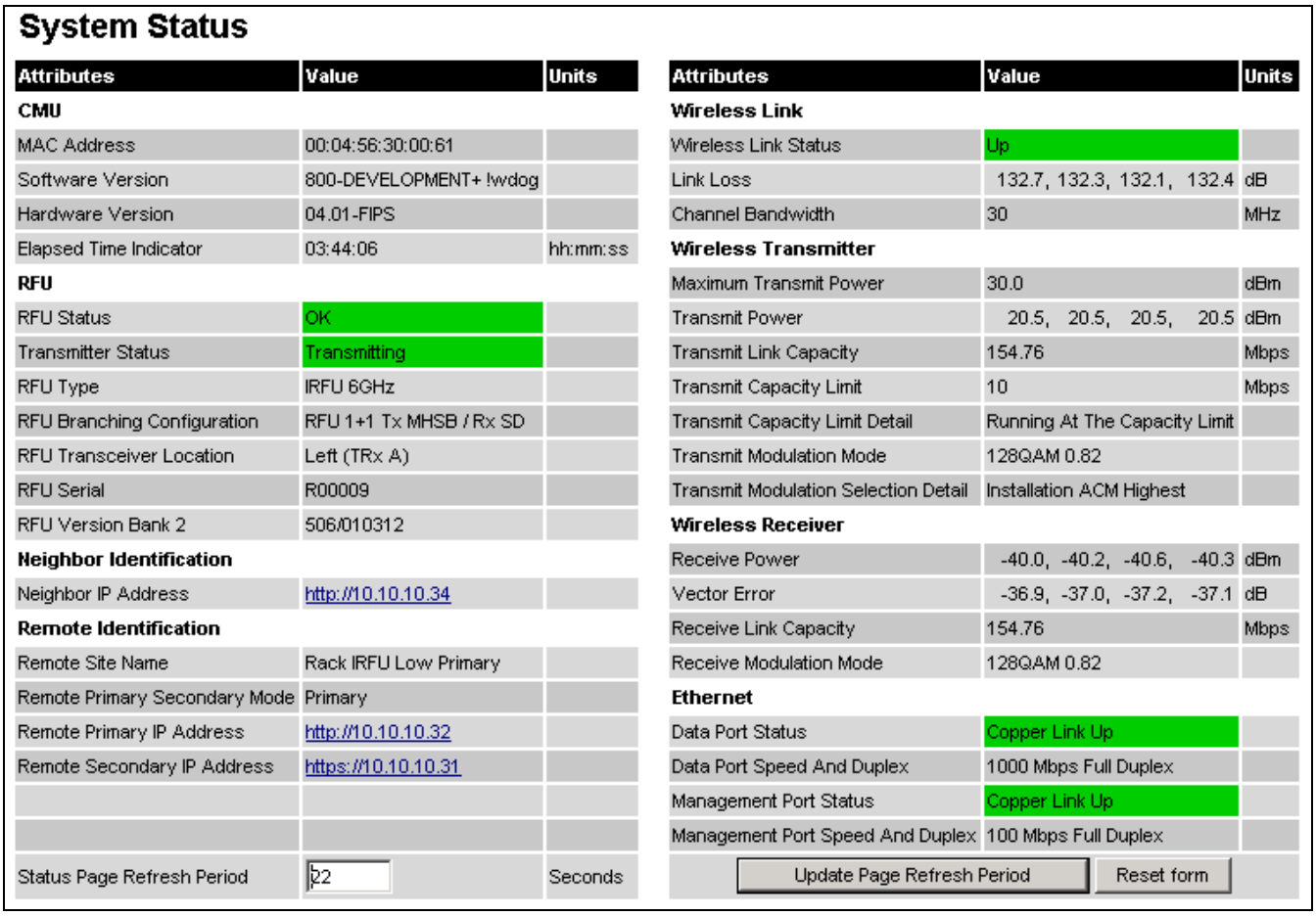
NOTE

Transmit power, receive power, vector error and link loss are presented as an array of four elements. These elements represent the maximum, mean, minimum and latest values respectively. The maximum, mean and minimum are calculated over a running one hour period.

Status page for 1+1 Hot Standby links

For a 1+1 protection scheme, the IP addresses of the neighboring PTP 800 and the two remote PTP 800s are displayed on the System Status page (Figure 183). If the IP address is shown then this is an active link to the GUI of the other PTP 800 and clicking it transfers access to the GUI of the other PTP 800. The full status of the protection is shown by the Protected Link screen, Managing 1+1 Hot Standby links on page 7-33.

Figure 183 System Status page (1+1 Hot Standby link)



System Status

Attributes	Value	Units
CMU		
MAC Address	00:04:56:30:00:61	
Software Version	800-DEVELOPMENT+ !wdog	
Hardware Version	04.01-FIPS	
Elapsed Time Indicator	03:44:06	hh:mm:ss
RFU		
RFU Status	OK	
Transmitter Status	Transmitting	
RFU Type	IRFU 6GHz	
RFU Branching Configuration	RFU 1+1 Tx MHSB / Rx SD	
RFU Transceiver Location	Left (TRx A)	
RFU Serial	R00009	
RFU Version Bank 2	506/010312	
Neighbor Identification		
Neighbor IP Address	http://10.10.10.34	
Remote Identification		
Remote Site Name	Rack IRFU Low Primary	
Remote Primary Secondary Mode	Primary	
Remote Primary IP Address	http://10.10.10.32	
Remote Secondary IP Address	https://10.10.10.31	
Status Page Refresh Period	22	Seconds

Attributes	Value	Units
Wireless Link		
Wireless Link Status	Up	
Link Loss	132.7, 132.3, 132.1, 132.4	dB
Channel Bandwidth	30	MHz
Wireless Transmitter		
Maximum Transmit Power	30.0	dBm
Transmit Power	20.5, 20.5, 20.5, 20.5	dBm
Transmit Link Capacity	154.76	Mbps
Transmit Capacity Limit	10	Mbps
Transmit Capacity Limit Detail	Running At The Capacity Limit	
Transmit Modulation Mode	128QAM 0.82	
Transmit Modulation Selection Detail	Installation ACM Highest	
Wireless Receiver		
Receive Power	-40.0, -40.2, -40.6, -40.3	dBm
Vector Error	-36.9, -37.0, -37.2, -37.1	dB
Receive Link Capacity	154.76	Mbps
Receive Modulation Mode	128QAM 0.82	
Ethernet		
Data Port Status	Copper Link Up	
Data Port Speed And Duplex	1000 Mbps Full Duplex	
Management Port Status	Copper Link Up	
Management Port Speed And Duplex	100 Mbps Full Duplex	

Update Page Refresh Period | Reset form

Status attributes

The System Status page contains a number of status attributes. These are highlighted in green for normal operation, or in red to indicate abnormal operation. The following status attributes are defined:

- RFU Status (Table 252).
- Transmitter Status (Table 253).
- Wireless Link Status (Table 254).
- Transmit Modulation Selection Detail Status (Table 255).
- Data Port Status (Table 256).
- Management Port Status (Table 257).

Table 252 RFU Status attribute values

Value	Meaning
OK	The RFU is ready for use.
RFU Fault	The RFU has raised alarms, but the CMU makes its best effort to carry on.
Incompatible License	The configured radio license is not compatible with this RFU. The RFU remains muted.
In Reset	The RFU is booting. This state is transient during CMU boot or after firmware download.
Download In Progress	New RFU firmware is being downloaded. Percentage completion is shown here.
Incompatible Firmware Version	The RFU firmware is too old. If possible, download will begin.
Incompatible Device	The connected device is an RFU, but it is not a Cambium branded product.
IF Card Attached	The connected device is an IF card, not an RFU.
No Response	No response can be detected from the RFU. It is probably not connected.
Power Supply Fault	The power supply to the RFU is at fault (short circuited).
Power Supply Disabled	The power supply to the RFU is disabled. It can only be enabled by Cambium.

Table 253 Transmitter Status attribute values

Value	Meaning
Transmitting	Normal transmission is in progress.
Inactive	The RFU is mute because it is in the inactive mode.
Muted - By User	The user has disabled transmission using the Configuration Page.
Muted - Configuration Error	The transmission is enabled but the radio license is not compatible.
Muted - RFU Fault	Transmission is enabled but an RFU fault is preventing transmission.

Table 254 Wireless Link Status attribute values

Value	Meaning
Up	The point-to-point link is established
Searching	A red background with status text “searching” indicates that the link is not established and no signal has yet been detected from the PTP 800 at the other end of the link. This is a valid status value; if the link remains in this state it implies that the remote PTP 800 has not been detected.
Other values	A red background with status text (registering, acquiring, initialising) indicates that the link is not yet established. These are normal stages in the establishment of an operational link. If the link remains in any state for a long period of time it implies a problem with the PTP 800.

Table 255 Transmit Modulation Selection Detail attribute values

Value	Meaning
Acquiring Link	The wireless link is not established.
Fixed	The Transmit Modulation Selection is set to ‘Fixed’.
Installation ACM Highest	The highest transmit modulation that can be used for the installation settings.
Installation ACM Lowest	The lowest transmit modulation that can be used for the installation settings.
User ACM Highest	The transmit modulation is the highest configured by the user.
User ACM Lowest	The transmit modulation is the lowest configured by the user.
Limited by wireless channel conditions	The transmit modulation is limited by the wireless conditions.

Table 256 Data Port Status attribute values

Value	Meaning
Down	The data port is not in operation.
Copper Link Up	The copper data port is operating normally.
Fiber Link Up	The fiber data port is operating normally.
Fiber-Y Standby	The PTP 800 is in standby mode in a 1+1 Hot Standby link with a Fiber-Y configuration.

Table 257 Management Port Status attribute values

Value	Meaning
Down	The management port is not in operation.
Copper Link Up	The copper management port is operating normally.

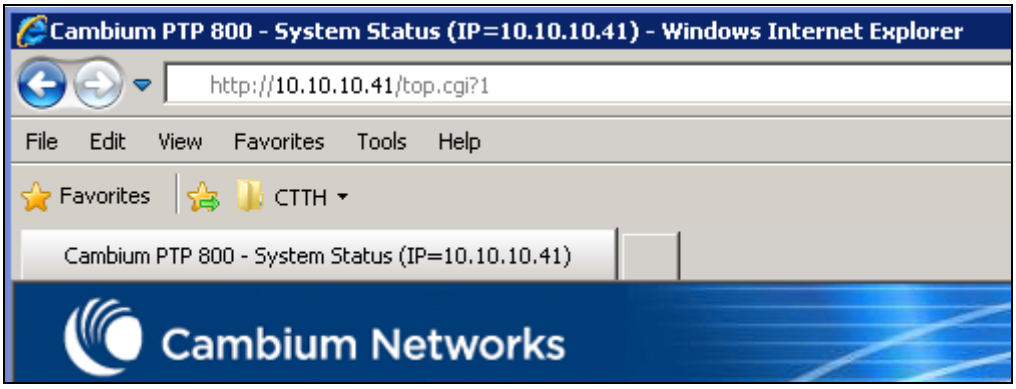
Identifying a unit from the web browser title

By default, the web browser title displays the following text:

Cambium PTP 800 - <current page> (IP = <ipAddress>)

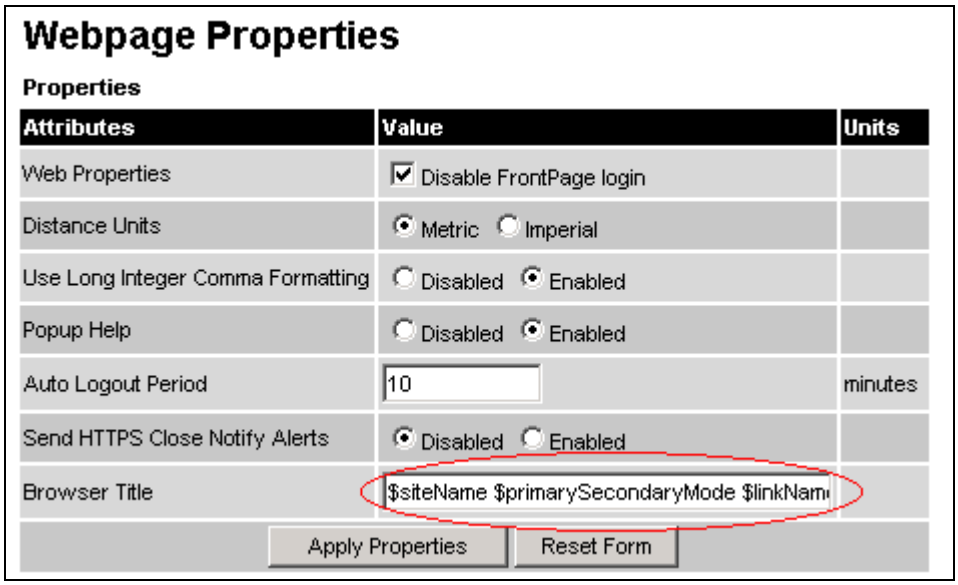
For example, if the IP address is 10.10.10.41 and the current page is the System Status page, the browser title is displayed as shown in Figure 184.

Figure 184 Web browser with default title


Cambium PTP 800 - System Status (IP=10.10.10.41) - Windows Internet Explorer
http://10.10.10.41/top.cgi?1
File Edit View Favorites Tools Help
Favorites
CTTH
Cambium PTP 800 - System Status (IP=10.10.10.41)
Cambium Networks

To configure the web browser such that units can be individually identified from the browser and tab titles, select menu option **Management, Web, Web Properties**. The Webpage Properties page is displayed (Figure 185). Update the Browser Title attribute (a blank entry will display the default title). Select **Apply Properties**.

Figure 185 Browser Title variable entry



In the Browser Title attribute, enter simple text and optional variables (prefixed with a $ character). The full list of variables is in Table 258.

Table 258 Browser Title attribute variables

Variable	Meaning
$siteName	Site name.
$linkName	Link name.
$primarySecondaryMode	Whether unit is configured as Primary or Secondary in 1+1 Hot Standby link.
$transmitHiLo	Whether unit is Tx Hi or Tx Lo.
$ipAddress	IP address of the CMU.
$sysName	Sys Name which is a part of the SNMP configuration.
$productName	This is a fixed value of Cambium PTP 800.
$pageName	Name of the page currently being browsed.

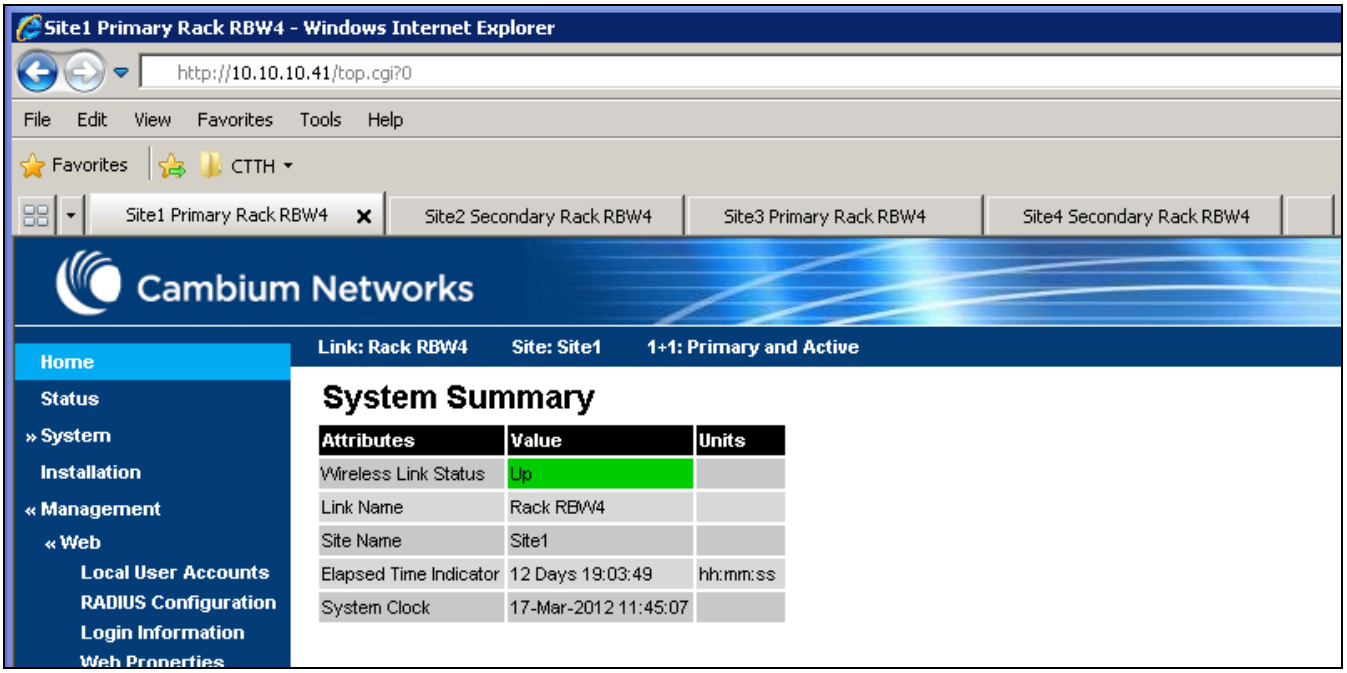
Example

Each unit in a 1+1 Hot Standby link may be fully identified by the siteName, the primarySecondaryMode and the linkName. For example, suppose that these variables are set to:

- siteName = ‘Site1’, ‘Site2’, ‘Site3’ and ‘Site4’
- primarySecondaryMode = ‘Primary’ or ‘Secondary’
- linkName = ‘Rack RBW4’

For each unit, use the Webpage Properties page to enter the relevant Browser Title variables (Figure 185). As a result, the four units in the 1+1 Hot Standby are identified in the browser tabs, and the currently selected unit is identified in the browser title bar (Figure 186).

Figure 186 Identifying units in the web browser title bar and tabs



Logging out

To maintain security, always log out at the end of a session by selecting menu option **Logout**.

Alternatively, the unit will log out automatically, but this depends upon the setting of Auto Logout Period in the Webpage Properties page (Figure 134).

Managing alarms and events

This section describes how to manage PTP 800 system alarms and events.

This section contains the following procedures:

- Managing alarms on page 7-15.
- Managing email alerts on page 7-24.
- Managing SNMP traps on page 7-24.
- Managing event notification messages on page 7-31.

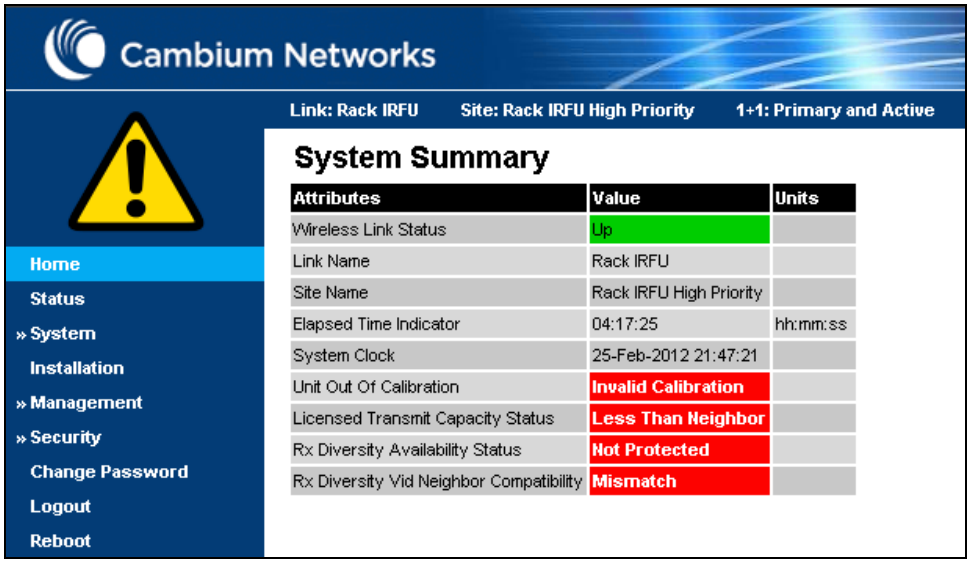
Managing alarms

Whenever system alarms are outstanding, a yellow warning triangle is displayed on the navigation bar. The warning triangle is visible from all web pages. Click the warning triangle (or menu option **Home**) to return to the System Summary page and view the alarms. If the warning triangle disappears when it is clicked, it indicates that the outstanding alarms have been cleared. A change of state in most alarms generates an SNMP trap or an SMTP email alert.

The alarm configuration procedure is described in Task 9: Configuring alarms and messages on page 6-90.

The example in Figure 187 shows the warning triangle in the navigation bar and the 'Channel A' alarm displayed in the System Summary page.

Figure 187 Alarm warning triangle



The alarms are defined as follows:

<attribute name> Neighbor Compatibility

Definition: In order for a 1+1 Hot Standby link end to be correctly protected, a number of key attributes must be configured to be compatible in the two neighbor CMUs. If a key attribute is configured to be mismatched, an associated alarm will be displayed on the Home page of both neighbor CMUs. Each alarm has the form <attribute name> neighbor compatibility, for example 'Radio License Tx Freq Neighbor Compatibility' indicates that the Radio License Tx Freq is different for the neighbor CMUs.

Cause and action: Correct the attribute which is indicating the mismatch.

Alignment mode

Definition: The CMU is in alignment mode.

Cause and action: This should only occur during installation or maintenance when the wireless link is being aligned. To take a unit out of alignment mode, access the Installation Wizard (see Task 7: Configuring wireless interface on page 6-63).

Data port configuration mismatch

Definition: The Ethernet configuration of the data port is not compatible with the connected network equipment.

Cause and action: This is probably due to a configuration error such as an auto-negotiation or forced configuration mismatch.

Data port disabled warning

Definition: The fiber and copper data port has been disabled by means of the SNMP MIB.

Cause and action: The port has been disabled by a network management system. The web browser provides no means of disabling this port.

Data Port Ethernet Speed Status

Definition: In a 1+1 Hot Standby configuration, this indicates if the Ethernet Speed of the Data port is below that of its neighbor. For example, where the Data Port has negotiated at 100BASE-T but the neighbor has negotiated at 1000BASE-T.

Cause and action: This could be due to a difference between the configuration of the Data ports of the neighbor CMUs (see LAN Configuration page) or in the configuration of the two ports at the network equipment. A fault in the Ethernet cable could also cause an Ethernet port to negotiate at a lower speed.

Data port fiber status

Definition: Reports the status of the fiber data port.

Cause and action: There are two possible causes:

- The interface could not be established even though a fiber carrier was detected. This could be due to a broken TX fiber, or because the interface is disabled at the other end of the fiber link.
- The interface could not be established and no fiber carrier is detected.

Data port status

Definition: The status of the data port, either fiber or copper link.

Cause and action: See Table 256 for values and their meanings.

Encryption Enabled Mismatch

Definition: Encryption has been enabled on one end of the wireless link but not the other.

Cause and action: This is probably due to an encryption configuration error. Reconfigure encryption.

End Wireless Receive Signal Status

Definition: This indicates if the end, consisting of two neighbor CMUs and two neighbor RFUs, are able to demodulate the transmit signal from the remote end of the link. For a 1+1 Hot Standby link with Rx Diversity enabled, both neighbors must be unable to demodulate the signal before this indicates a value of Not Detected. For 1+1 Hot Standby link where Rx Diversity is disabled, this indicates a value of Not Detected only if the active CMU cannot demodulate the signal.

Cause and action: If this alarm is unaccompanied by other alarms, the cause will often be due to a deep fade of the wireless channel. This could be caused by many environmental effects such as rain fades in the higher frequency bands or ducting for long links where Spatial Rx Diversity is not deployed.

FCC capacity check

Definition: The Transmit Capacity Limit of the unit (lower of license key and negotiated Ethernet speed at remote end) is below the appropriate level required by FCC Part 101.141.

Cause and action: This is probably due to a configuration error or the wrong license being applied to one of the CMUs.

Fips Operational Mode Alarm

Definition: The unit is FIPS 140-2 capable, but has not been configured correctly for FIPS 140-2 operation.

Cause and action:

- 'FIPS mode is not configured': The Security Wizard has not been completed.
- 'FIPS mode is configured, but not active': The Security Wizard has been completed, but the HTTP and Telnet management interfaces have not been disabled.

Licensed Transmit Capacity Status

Definition: In a 1+1 Hot Standby configuration, this indicates that the Licensed Transmit Capacity is below that of its neighbor.

Cause and action: This is probably due to a configuration error or the wrong license being applied to one of the CMUs.

Link name mismatch

Definition: The link names at each end of the wireless link do not match.

Cause and action: The link name is configured differently at each end of the wireless link. This may be because of:

- A configuration error in defining the link name at one of the PTP 800s, see Step 1: Enter equipment details on page 6-65;
- This unit is aligned to the wrong link partner.

Management port configuration mismatch

Definition: The Ethernet configuration of the management port is not compatible with the connected network equipment.

Cause and action: This is probably due to a configuration error such as an auto-negotiation or forced configuration mismatch. See Configuring the IP interface and management mode on page 6-10.

Management port disabled warning

Definition: The management port has been disabled by means of the SNMP MIB.

Cause and action: The port has been disabled by a network management system. The web browser provides no means of disabling this port.

Management Port Ethernet Speed Status

Definition: In a 1+1 Hot Standby configuration, this indicates if the Ethernet Speed of the Management port is below that of its neighbor. For example, where the Management port has negotiated at 10BASE-T but the neighbor has negotiated at 100BASE-T.

Cause and action: This could be due to a difference between the configuration of the Management ports of the neighbor CMUs (see LAN configuration page) or in the configuration of the two ports at the network equipment. A fault in the Ethernet cable could also cause an Ethernet port to negotiate at a lower speed.

Management port status

Definition: The status of the management port if out-of-band management is being used.

Cause and action: See Table 257 for values and their meanings.

Protection Availability Status

Definition: This indicates if an end of a 1+1 Hot Standby link is not protected, for example due to the inactive unit exhibiting a fault, the protection cable being disconnected, the configuration of the inactive unit being incompatible with that of the active unit, or Fault Protection Switching being set to disabled. If the end is not protected, the active unit will indicate 'Not Protected' and the inactive unit will indicate ‘Not Protecting’.

Cause and action: If a unit is indicating that it is not protected or not protecting, check the following:

- Check that the configuration of the two neighbors is compatible. See <attribute name> neighbor compatibility.
- Check that the transmitter of the inactive unit is not muted. This is controlled on the Configuration page or the Protection Page.
- Check that the two neighbors are not in Alignment Mode (See Alignment Mode (top of this table)).
- Check that Fault Protection Switching is Enabled. This can be set from the Protection Configuration page or the Protected Link Management page.
- Check that the Protection Interface is operating correctly (see Protection Interface Status)
- Check that the inactive unit is not exhibiting any faults.

Protection Interface Status

Definition:

- If the protection cable is physically disconnected from either CMU, this indicates ‘Not Connected’.
- If the protection cable is connected at both neighbor CMUs but the neighbor is not responding, this indicates ‘Neighbor Not Responding’.

Cause and action:

- If indicating ‘Not Connected’ check that the protection cable is physically connected at both CMUs. If installed, check the cabling to the OOB Protection Splitter.
- If indicating ‘Neighbor Not Responding’ check the following:
  - Check that the neighbor CMU is powered up and functioning.
  - Check that Protection has been configured as 'Protection 1+1' - see Protection Configuration page.
  - Check the integrity of the protection cables.

RFU Common IF Synth Lock

Definition: This indicates a failure of the Common IF synthesizer in the RFU.

Cause and action: This is a failure of the RFU hardware. Please inform Customer Support of this alarm.

RFU Common RF Synth Lock

Definition: This indicates a failure of the Common RF synthesizer in the RFU.

Cause and action: This is a failure of the RFU hardware. Please inform Customer Support of this alarm.

RFU Fan

Definition: This indicates when the IRFU transceiver fan assembly has failed. The assembly consists of two fans and if one fan fails, the this will report partial failure. If both fans fail, this will report total failure.

Cause and action: This is a failure of the IRFU fan assembly. Please inform Customer Support of this alarm.

RFU High Temperature

Definition: This indicates when the temperature of the IRFU transceiver has risen above either of two thresholds:

- If the temperature exceeds the High Temperature threshold, the transmit power may reduce.
- If the temperature exceeds the Very High Temperature threshold, the transceiver will mute the transmitter.

Cause and action: This could be caused by failure of the IRFU transceiver fan assembly. Check if there is an active fan alarm:

- If there is no active fan alarm, check that there is nothing obstructing the correct operation of the fan assembly.
- If nothing is obstructing the fan assembly, ensure that the IRFU has been installed correctly and in an environment which is in line with specifications.

RFU RF Switch

Definition: For a 1+1 IRFU, both the Primary and Secondary transceivers transmit but the energy from only one of the transceivers is switched to the antenna via an RF switch. The RF switch resides in the branching unit of the IRFU. This alarm is displayed if the RF switch fails to switch.

Cause and action: The most likely cause is a failure of the IRFU RF Switch. Please inform Customer Support of this alarm.

RFU RF Switch Cable

Definition: For a 1+1 IRFU, both the Primary and Secondary transceivers transmit but the energy from only one of the transceivers is switched to the antenna via an RF switch. The RF switch resides in the branching unit of the IRFU and connects to each transceiver with a separate cable. This alarm is raised if the transceiver cannot detect the RF Switch.

Cause and action: The most likely cause is that the cable connecting the transceiver to the RF switch is faulty or disconnected.

RFU Rx IF Synth Lock

Definition: This indicates a failure of the Rx IF synthesizer in the RFU.

Cause and action: This is a failure of the RFU hardware. Please inform Customer Support of this alarm.

RFU Rx RF Synth Lock

Definition: This indicates a failure of the Rx RF synthesizer in the RFU.

Cause and action: This is a failure of the RFU hardware. Please inform Customer Support of this alarm.

RFU Status

Definition: The status of the RFU.

Cause and action: The possible values for this attribute are shown in Table 252. If the value is set to Fault, there will be another RFU alarm condition displayed indicating the detail of the fault.

RFU Tx IF Synth Lock

Definition: This indicates a failure of the Tx IF synthesizer in the RFU.

Cause and action: This is a failure of the RFU hardware. Please inform Customer Support of this alarm.

RFU Tx RF Synth Lock

Definition: This indicates a failure of the Tx RF synthesizer in the RFU.

Cause and action: This is a failure of the RFU hardware. Please inform Customer Support of this alarm.

Rx Diversity Availability Status

Definition: Receive Diversity is enabled but not operating.

Cause and action:

- The Inactive CMU is not operating. Check that it is powered up and can be managed.
- The neighbor CMU does not have Rx Diversity enabled. Check the value of the protection attribute.
- The neighbor CMUs are configured with incompatible attribute values. Check for any outstanding configuration attributes <attribute Name> Neigbor Compatibility and correct the mismatch.
- The RFU of the Inactive unit is faulty or not responding to the CMU. Check that there is no outstanding RFU Status alarm.
- The IF cable between Inactive CMU and RFU is faulty. Check that there is no outstanding RFU Status alarm.
- The Protection Interface is not operating. Check that there is no outstanding Protection Interface Status alarm.

- The Data Port of either CMU is not connected or has not negotiated at 1000 Mbps. Check that there is no outstanding Rx Diversity Data Port Status alarm on either CMU.
- If none of the above conditions exist but Rx Diversity Availability is still indicating a problem, the likely cause is the configuration of the Rx Diversity VLAN in the Ethernet Switch. Check that the Ethernet Switch is configured correctly to ensure that Rx Diversity Ethernet Frames are bridged between the Inactive and Active.

Rx Diversity Data Port Status

Definition: For Rx Diversity to operate, the Data Port of both the Active and Inactive CMU must be negotiated at 1000 Mbps. This attribute is displayed if this is not the case.

Cause and action:

- There is a problem with the Ethernet Cable. Check that the Data Port Status of both neighbor CMUs is indicating that the port has negotiated at 1000 Mbps Full Duplex.
- The Active or Inactive CMU has been configured to prevent operation at 1000 Mbps. Check that the Data Port Copper Auto Negotiation is set to enabled and that Data Port Copper Auto Neg Advertisement includes 1000 Mbps Full Duplex. These are available on the LAN Configuration page.
- The Ethernet Switch is configured to prevent operation at 1000 Mbps.
- If operating with Fiber-Y,the Data Port of the Inactive CMU has trained with fiber. This is incorrect for Fiber-Y. Check that the value of Data Port Status is set to Copper Link Up. This is displayed on the Status Page. If this is not the case, check that copper Data Port is also connected to the Ethernet Switch as well as the Fiber-Y cable.

SNTP Synchronization Failed

Definition: SNTP has been enabled but the unit is unable to synchronize with the specified SNTP server.

Cause and action: If SNTP Sync fails then check the server settings or disable SNTP and set the time locally. See Setting the real-time clock on page 6-115.

Unit Out Of Calibration

Definition: The unit is out of calibration and must be returned to the factory using the RMA process for re-calibration.

Cause and action: Check the calibration status and arrange for recalibration of the unit.

Wireless link status

Definition: The status of the end-to-end wireless link.

Cause and action: See Table 254 for values and their meanings.

Wireless Receive Signal Status

Definition: The Wireless Receive Signal Status indicates if the receiver is able to demodulate the transmit signal from the remote end of the link.

Cause and action: If this alarm is unaccompanied by other alarms, the cause will often be due to a deep fade of the wireless channel. This could be caused by many environmental effects such as rain fades in the higher frequency bands or ducting for long links.

Managing email alerts

The management agent can be configured to generate alerts by electronic mail when certain events occur. The email message configuration procedure is described in Task 9: Configuring alarms and messages on page 6-90. The alerts mirror the SNMP traps defined in Table 259.

Managing SNMP traps

The PTP 800 supports SNMP v2 remote management and provides a comprehensive range of alarms. Table 259 lists the SNMP traps that the PTP 800 supports, their significance and possible causes.

The SNMP configuration procedure is described in Task 9: Configuring alarms and messages on page 6-90. The traps may be disabled totally or individual traps disabled.

> **NOTE**
> These traps mirror the system status and alarm information displayed on the System Summary and System Status pages.

Table 259 SNMP traps supported by PTP 800

SNMP Trap name	Description	Cause and action
MIB2 traps		
coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	The CMU has rebooted. See Rebooting on page 7-69.

SNMP Trap name	Description	Cause and action
linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the Operational Status for one of its communication links is about to enter the down state from some other state.	The link has gone down. This may be due to: Problems with the PTP 800. Problems on the link itself Failure of a device at the other end of the link.
linkUp	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the Operational Status for one of its communication links left the down state and transitioned into some other state – normally up.	The link is now available for service.
protectionStateTrap	In a 1+1 Hot Standby link, this trap is sent to indicate a change in the protectionState of a unit from active to inactive or vice versa.	A protection switch may have occurred due to a fault. Check for faults on the newly inactive unit. The protectionState trap is also sent when a unit initializes.
Diagnostic alarms		
alignmentModeTrap	Indicates if the unit is undergoing alignment. A change of state during operation may generate an SNMP trap and/or SMTP email alert.	This should only occur during installation or maintenance when the wireless link is being aligned.
linkNameMismatchTrap	Signaling was received with the wrong Link Name.	The link name is configured differently at each end of the wireless link. This may be because of: A configuration error in defining the link name at one of the PTP 800s. This unit is aligned to the wrong link partner.

SNMP Trap name	Description	Cause and action
unitOutOfCalibration Trap	The unit is out of calibration.	Check the calibration status and arrange for re-calibration of the unit.
encryptionEnabledMismatchTrap	Encryption has been enabled on one end of the wireless link but not the other.	Configuration error in defining use of encryption over the wireless link.
sNTPSyncTrap	The PTP 800 has failed to synchronize its time with the SNTP server.	If SNTP Sync fails then check the server settings in the Remote Management page, or disable SNTP and set the time locally. See Setting the real-time clock on page 6-115.
wirelessLinkStatusTrap	The status of the wireless link has changed.	This shows the status that the wireless link has entered. If the link remains in the state 'registering' or 'searching' it is unable to detect the PTP 800 at the other end of the link. This may be due to the unit at the other end of the link not being operational, being incorrectly configured/aligned or due to adverse weather conditions.
dataPortConfigurationMismatchTrap	The detection of Ethernet fragments (runt packets) on the data Ethernet port when the link is in full duplex operation.	This is probably due to a configuration error such as an auto-negotiation or forced configuration mismatch.
dataPortDisabledWarningTrap	The Administrative Status of the data Ethernet interface has been set to disabled.	The Ethernet data port has been disabled remotely by a management system. The physical port continues to remain operational but no data is transmitted.

SNMP Trap name	Description	Cause and action
dataPortFiberStatusTrap	A problem has been detected with the fiber interface on the data Ethernet port. The attribute dataPotrtFiberStatus identifies which problem has been detected.	There are three possible causes: 1) The fiber interface has been installed but disabled (because the license key does not include fiber support). 2) The interface could not be established even though a fiber carrier was detected. This could be due to a broken TX fiber, or because the interface is disabled at the other end of the fiber link. 3) The interface could not be established and no fiber carrier is detected.
managementPortConfigurationMismatchTrap	The detection of Ethernet fragments (runt packets) on the data Ethernet port when the link is in full duplex operation.	This is probably due to a configuration error such as an auto-negotiation or forced configuration mismatch.
managementPortDisabledWarningTrap	The Administrative Status of the out-of-band management Ethernet interface has disabled Ethernet traffic.	The management Ethernet port has been disabled remotely by a management system. Note that the physical port continues to operate but no data is transmitted over it.
rFUStatusTrap	A change of status of the RFU has occurred.	The RFU Status indicates the nature of the RFU fault. A state of 'ok' indicates that the RFU is fully operational, although may not be transmitting.
dataPortStatusTrap	A change of state for the data port has occurred.	The data port status has changed – most significantly to up or down

SNMP Trap name	Description	Cause and action
managementPortStatusTrap	Change of status of the out-of-band management Ethernet link. This may indicate a status of “down” or “copper link up”.	This may be due to failure of the link or equipment at the either end of the link. Note that a failure trap may not be received if no route is available.
protectionAvailabilityStatusTrap	This indicates that an end of a 1+1 Hot Standby link is not protected, for example due to the inactive unit exhibiting a fault, the protection cable being disconnected, the configuration of the Inactive unit being incompatible with that of the active unit or Fault Protection Switching being set to disabled. If the end is not protected, the active unit will indicate 'Not Protected' and the inactive unit will indicate ‘Not Protecting’.	If this trap is generated when a unit is not protected or not protecting, check the configuration of both units and check for alarms on the inactive unit. Check whether fault protection switching is enabled.
protectionConfigurationStatus	In order for a 1+1 Hot Standby link end to be correctly protected, a number of key attributes must be configured to be compatible in the two neighbor CMUs. If a key attribute is configured to be mismatched, a configurationProtectionStatus trap will be generated with a value of ‘Configuration Not Protecting’. A trap will be sent with a value of OK if the condition is cleared.	If a configurationProtectedStatus trap indicates that the configuration of the inactive unit is not protecting the active unit, log into the web interface of either unit and check which attribute is mismatched (see <attribute name> neighbor compatibility).
rxDiversityAvailabilityStatusTrap	Receive Diversity is enabled but not operating.	Refer to Rx Diversity Availability Status on page 7-22.

SNMP Trap name	Description	Cause and action
rxDiversityDataPortStatusTrap	For Rx Diversity to operate, the Data Port of both the Active and Inactive CMU must be negotiated at 1000 Mbps. This attribute is displayed if this is not the case.	Refer to Rx Diversity Data Port Status on page 7-23.
rxDiversityConfigurationStatusTrap	In order for Receive Diversity to operate correctly in a 1+1 Hot Standby link, a number of key attributes must be configured to be compatible in the two neighbor CMUs. If a key attribute is configured to be mismatched, this trap will be generated. A trap will be sent with a value of OK if the condition is cleared.	Log into the web interface of either unit and check which attribute is mismatched.
wirelessReceiveSignalStatusTrap	This trap is only issued for 1+1 Hot Standby configurations. The Wireless Receive Signal Status indicates if the receiver is able to demodulate the transmit signal from the remote end of the link. If it cannot demodulate the signal, a protection switch may occur.	This may be due to hardware problems: the RFU, antenna or CMU. It may also be due to incorrect configuration, or radio fading caused by adverse weather conditions.
endWirelessReceiveSignalStatusTrap	In a 1+1 Hot Standby configuration, this indicates if the end, consisting of two neighbor CMUs and two neighbor RFUs, is able to demodulate the transmit signal from the remote end of the link.	Refer to End Wireless Receive Signal Status on page 7-17.
licensedTransmitCapacityStatusTrap	In a 1+1 Hot Standby configuration, this indicates that the Licensed Transmit Capacity is below that of its neighbor.	This is probably due to a configuration error or the wrong license being applied to one of the CMUs.

SNMP Trap name	Description	Cause and action
dataPortEthernetSpeedStatusTrap	In a 1+1 Hot Standby configuration this indicates that the Ethernet Speed of the Data Port is below that of its neighbor.	This is probably due to a configuration error.
managementPortEthernetSpeedStatusTrap	In a 1+1 Hot Standby configuration, this indicates that attribute indicates that the Ethernet Speed of the Management Port is below that of its neighbor.	This is probably due to a configuration error.
protectionInterfaceStatusTrap	In a 1+1 Hot Standby configuration, information is shared between neighbor CMUs over the Protection Interface. This reports whether the neighbor CMU is successfully responding, physically disconnected or whether it is physically connected but not responding, for example powered down.	This may indicate that the other unit is faulty, not available or the protection interface is not installed, not working or disconnected.

Managing event notification messages

When system logging is enabled, log entries are added to the internal log and (optionally) transmitted as UDP messages to one or two syslog servers.

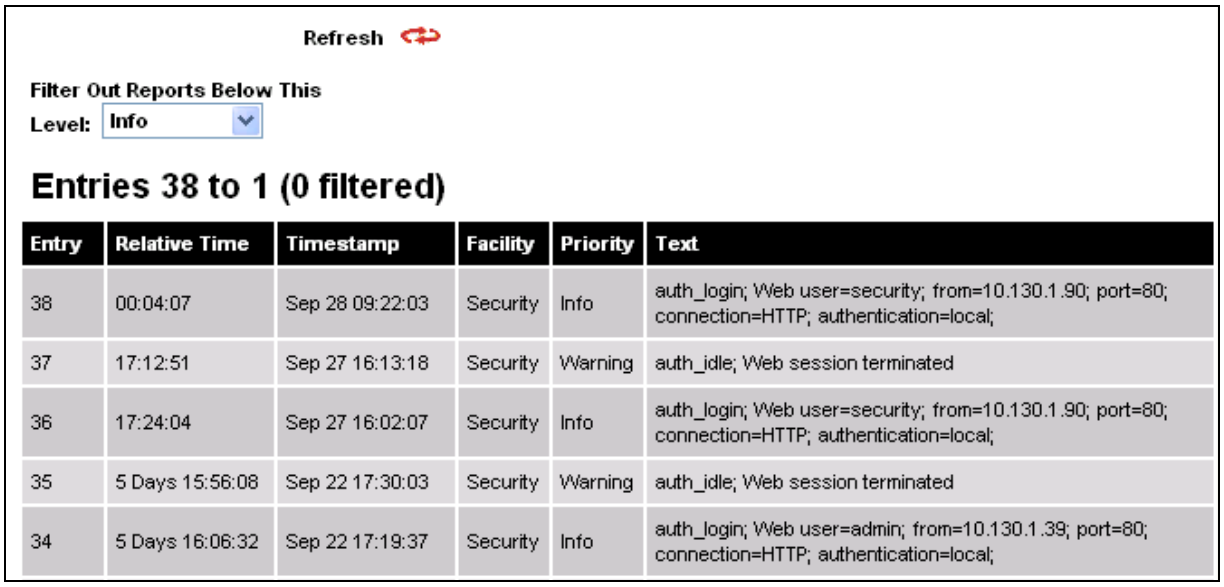
For more information about system logging, refer to:

- System logging (syslog) on page 1-59 describes the system logging feature.
- Syslog message formats on page 4-73 describes the format and content of syslog event messages.
- Task 10: Configuring syslog on page 6-94 describes the system logging configuration procedure.

To enable system logging, select menu option **Management, Syslog, Syslog configuration**. The Syslog Configuration page is displayed (Figure 164). Set the Syslog State attribute to 'Enabled'.

To view the log, select menu option **Management, Syslog**. The local log is displayed (Figure 188).

Figure 188 Syslog local log



Entry	Relative Time	Timestamp	Facility	Priority	Text
38	00:04:07	Sep 28 09:22:03	Security	Info	auth_login; Web user=security; from=10.130.1.90; port=80; connection=HTTP; authentication=local;
37	17:12:51	Sep 27 16:13:18	Security	Warning	auth_idle; Web session terminated
36	17:24:04	Sep 27 16:02:07	Security	Info	auth_login; Web user=security; from=10.130.1.90; port=80; connection=HTTP; authentication=local;
35	5 Days 15:56:08	Sep 22 17:30:03	Security	Warning	auth_idle; Web session terminated
34	5 Days 16:06:32	Sep 22 17:19:37	Security	Info	auth_login; Web user=admin; from=10.130.1.39; port=80; connection=HTTP; authentication=local;

Disabling and enabling the wireless interface

This section describes how to disable wireless transmission (prevent antenna radiation) and enable wireless transmission (allow antenna radiation).

Disabling wireless transmission

This is necessary when maintenance work is needed near the antenna. To disable wireless transmission, select menu option **Configuration**. The System Configuration page is displayed (Figure 172). Select **Mute Transmitter**. The Transmitter attribute value changes to 'Muted'.

NOTE

Wireless transmission can also be disabled from the Protection Configuration page (Figure 136), for both protected and unprotected links.

CAUTION

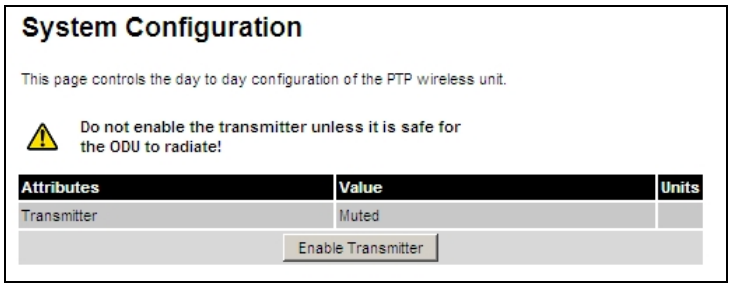
In a 1+1 Hot Standby link, disable protection switchover before disabling wireless transmission (see Enabling and disabling fault protection on page 7-43). Otherwise, a switchover to the inactive unit may occur when the wireless interface is muted. Re-enable protection switchover when wireless transmission is re-enabled.

Enabling wireless transmission

This is necessary to restart the link when maintenance work is complete. To enable wireless transmission, select menu option **Configuration**. The System Configuration page is displayed (Figure 189). Select **Enable Transmitter**. The Transmitter attribute value changes to 'Enabled'.

Wireless transmission can also be enabled from the Protection Configuration page (Figure 136), for both 1+1 Hot Standby and unprotected links.

Figure 189 System Configuration page (partial view) when transmitter is muted


System Configuration
This page controls the day to day configuration of the PTP wireless unit.
Do not enable the transmitter unless it is safe for the ODU to radiate!
Attributes
Value
Units
Transmitter
Muted
Enable Transmitter

Managing 1+1 Hot Standby links

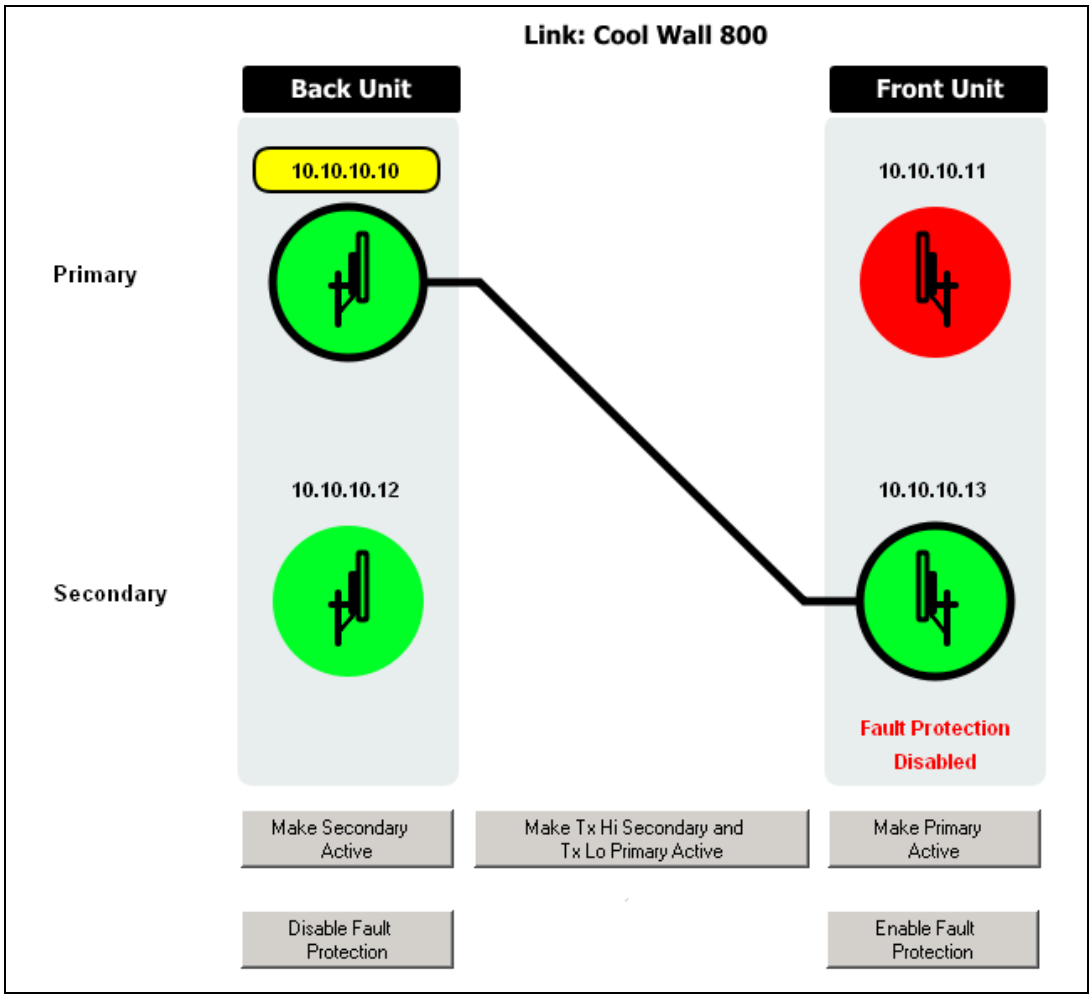
This section describes how to manage 1+1 Hot Standby links

> **NOTE**
> If a software upgrade is required, see Upgrading software in an operational 1+1 Hot Standby link on page 7-69.

Viewing the status of a 1+1 Hot Standby link

To view the status of a 1+1 Hot Standby link, select menu option **Configuration**, **Protected Link** (this option is only available when link protection is enabled). The Protected Link page (Figure 190) is displayed.

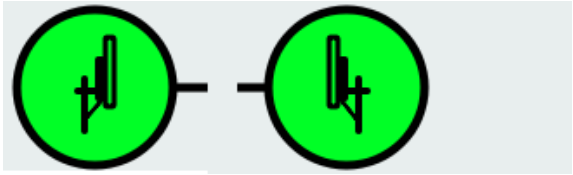
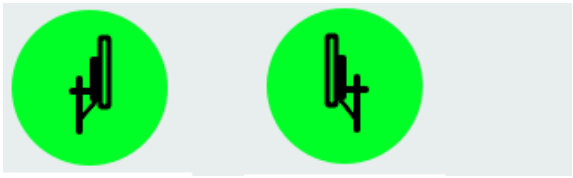
Figure 190 Protected Link page



This page shows the same view of the link from the web interface of any of the four units. The positions of the units on the page are determined by their Tx Hi/Lo and Primary/Secondary mode settings. The symbols, text and their meanings are shown in Table 260.

Table 260 Protected Link page symbols and text

Symbols or text	Meaning
Back Unit	Each end of the link is identified by a Site Name. The Site Name is configured using the Install Wizard or can be updated using the Configuration page. At a given end, it is recommended that the Site Name is configured to the same name for both Primary and Secondary CMUs. The end which is configured with the transmit frequency on the high side of the FDD frequency plan (Tx Hi) is always shown on the left. If no Site Name has been configured at either end, the labels will indicate Tx Hi or Tx Lo.
Primary	The CMU configured as Primary is the preferred unit in that it will become the active unit unless it is faulty. In the case where the two ODUs at an end have a different path loss, for example where they are coupled to a common antenna using an asymmetric coupler mounting kit (see Coupler mounting kits on page 1-30) , the CMU configured as Primary should be connected to the RFU with the lowest path loss. For IRFUs, the CMU configured as Primary should always be connected to the left hand transceiver.

Symbols or text	Meaning
Secondary	The CMU configured as Secondary will become the inactive unit unless the Primary unit develops a fault. In the case where the two ODUs at an end have a different path loss, for example where they are coupled to a common antenna using an Asymmetric Coupler Mounting Kit (see Coupler mounting kits on page 1-30) , the CMU configured as Secondary should be connected to the RFU with the highest path loss. For IRFUs, the CMU configured as Secondary should always be connected to the right hand transceiver.
10.10.10.10	The IP address of the unit being browsed.
10.10.10.12	The IP address of the unit.
	These units are active (Tx Hi and Tx Lo). Active units are the units which radiate at the antenna and forward traffic between the wireless interface and the Ethernet ports. The black line represents the link between active units.
	These units are inactive (Tx Hi and Tx Lo). Inactive units remain on standby waiting to take over the active role in case of a fault. They do not radiate or forward traffic between the Wireless interface and the Ethernet ports.
	These units are not protecting the active unit. They may be faulty or configured in a way which is not protecting the active unit. Roll the mouse over the icon to see the reason why the unit is not protecting.
	The unit being browsed cannot communicate with a unit identified in this way. This may be because the unit is powered down or the protection cable is not connected. If both units at the end remote from the end being managed are gray, this indicates that the wireless link is down.

Symbols or text	Meaning
Fault Protection Disabled	This indicates that fault protection is disabled by management. This prevents automatic protection switching on detection of a fault occurs. A managed protection switch can still be executed.

Using the Protected Link page

Viewing system status

To view the System Status page for an active, inactive or faulty unit, click on the icon. See Viewing the system status on page 7-7.

Viewing alarms and faults

If the alarm warning triangle is displayed on the menu bar, click on it to view the outstanding alarm list for the unit that currently provides the management interface. See Viewing the system summary on page 7-6 and Managing alarms on page 7-15.

Rolling the cursor over a red icon causes a list of protection faults for that unit to be displayed.

Viewing the status of mismatched neighbors

Certain configuration attributes must be the same on neighbors in order for an inactive unit to protect an active unit. If the inactive unit does not match, it will be shown in red on the Protected Link page and the reason will be ‘Configuration not protecting’. To determine which attribute is not matched, select the Home page of the misconfigured unit.

If the inactive unit is not protecting the active unit for any reason (for example, it is misconfigured or has a fault) a summary attribute called protectionAvailabilityStatus will be displayed on the Home page of both the active and inactive unit. On the active unit it will have the value of ‘Not Protected’. On the inactive unit it will have the value of ‘Not Protecting’.

Forcing protection switches

Protection switches may be forced for a variety of reasons, for example:

- During maintenance operations.
- During software or hardware upgrades.
- To investigate error conditions that have not resulted in a protection switch.
- To confirm that the inactive unit remains fully functional.

⚠ CAUTION

To avoid loss of service, force protection switches only if link planning indicates that the unit(s) are capable of operating a satisfactory link.

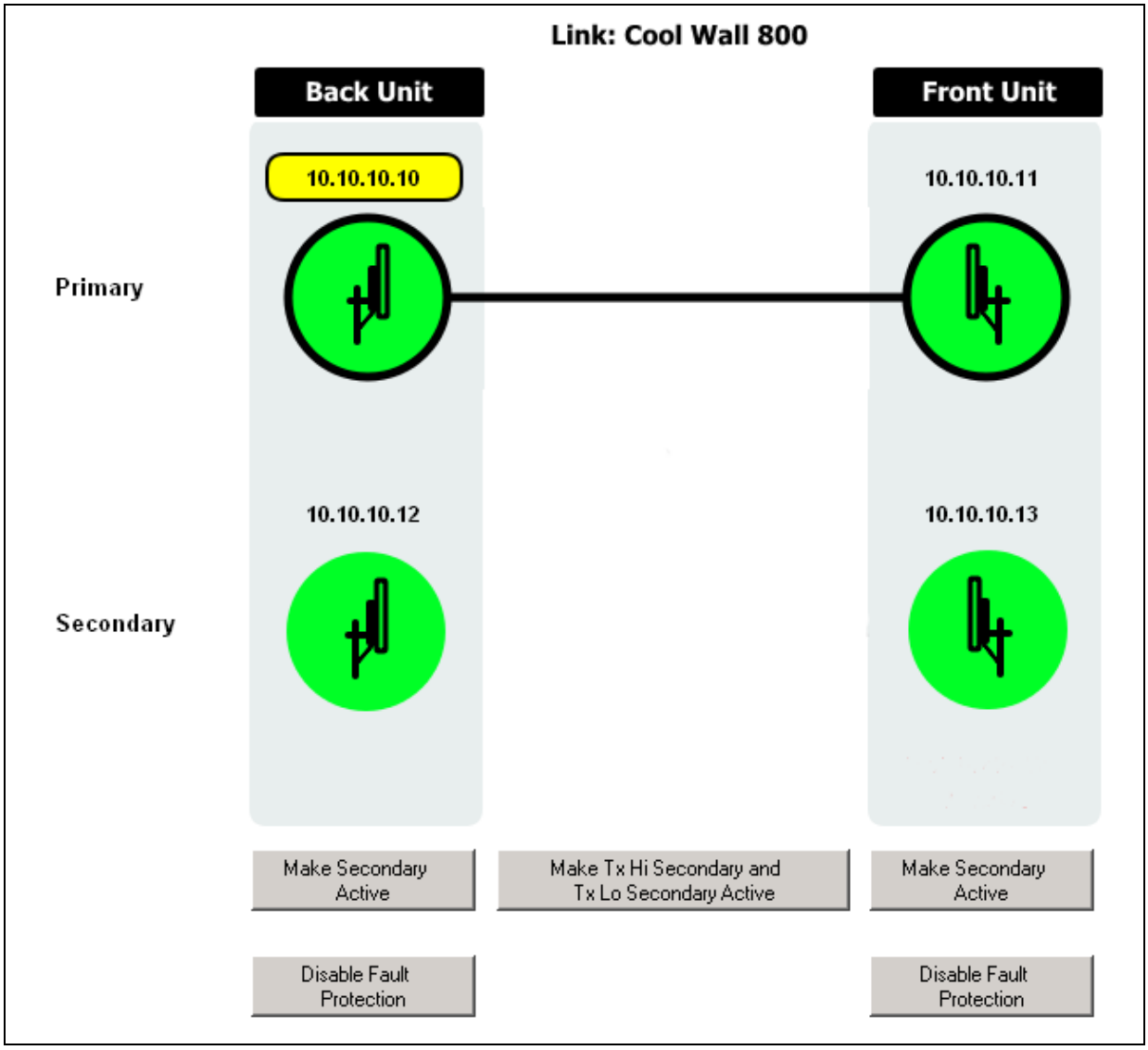
After a protection switch has been initiated, if work is to be carried out on the newly inactive unit, ensure that fault protection is temporarily disabled until the activity is completed.

To force protection switches, click on the buttons on the Protected Link page. The text in the buttons varies depending upon which units are active and which are inactive.

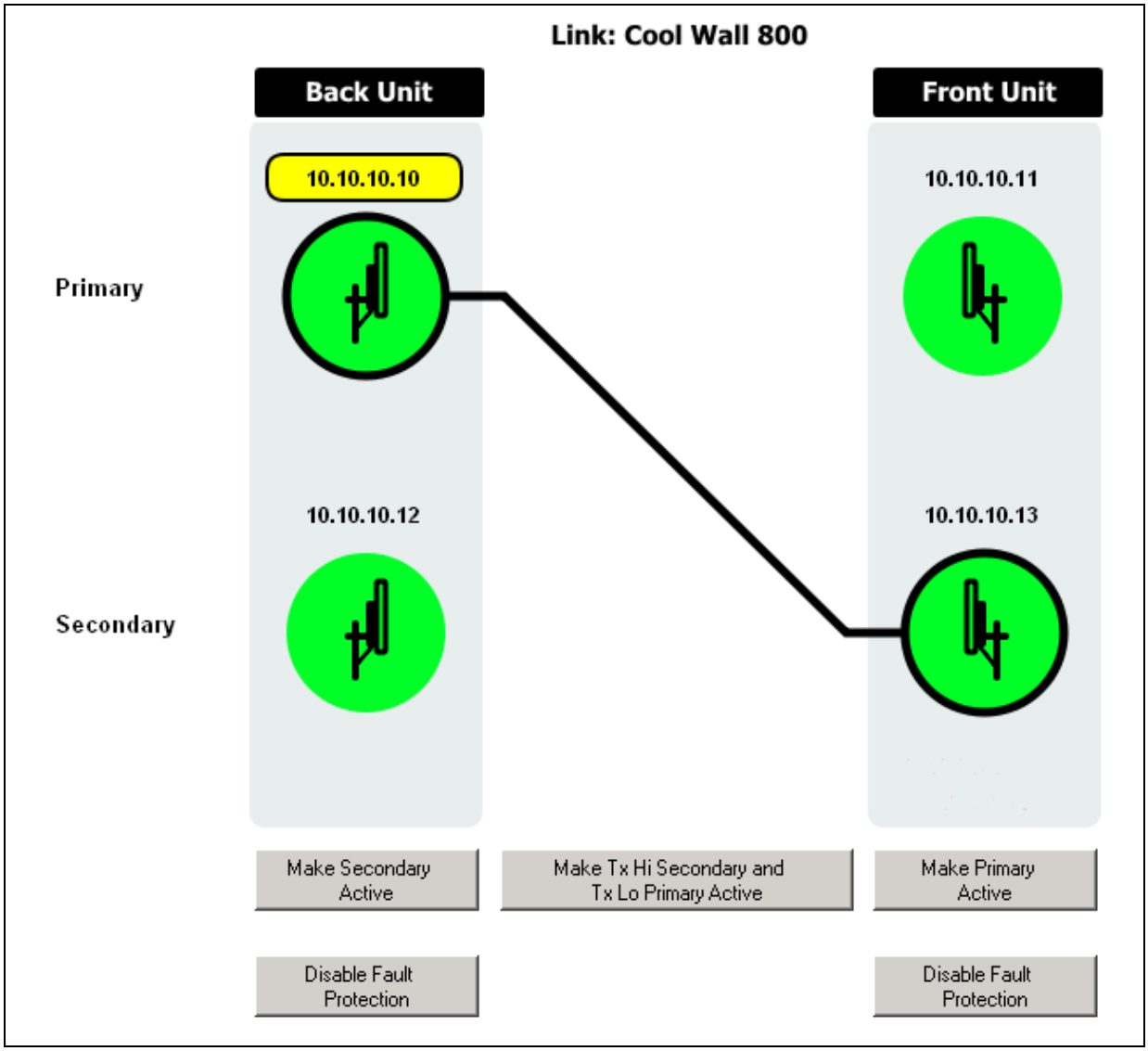
Example

For example, one possible forced protection switching sequence is as follows:

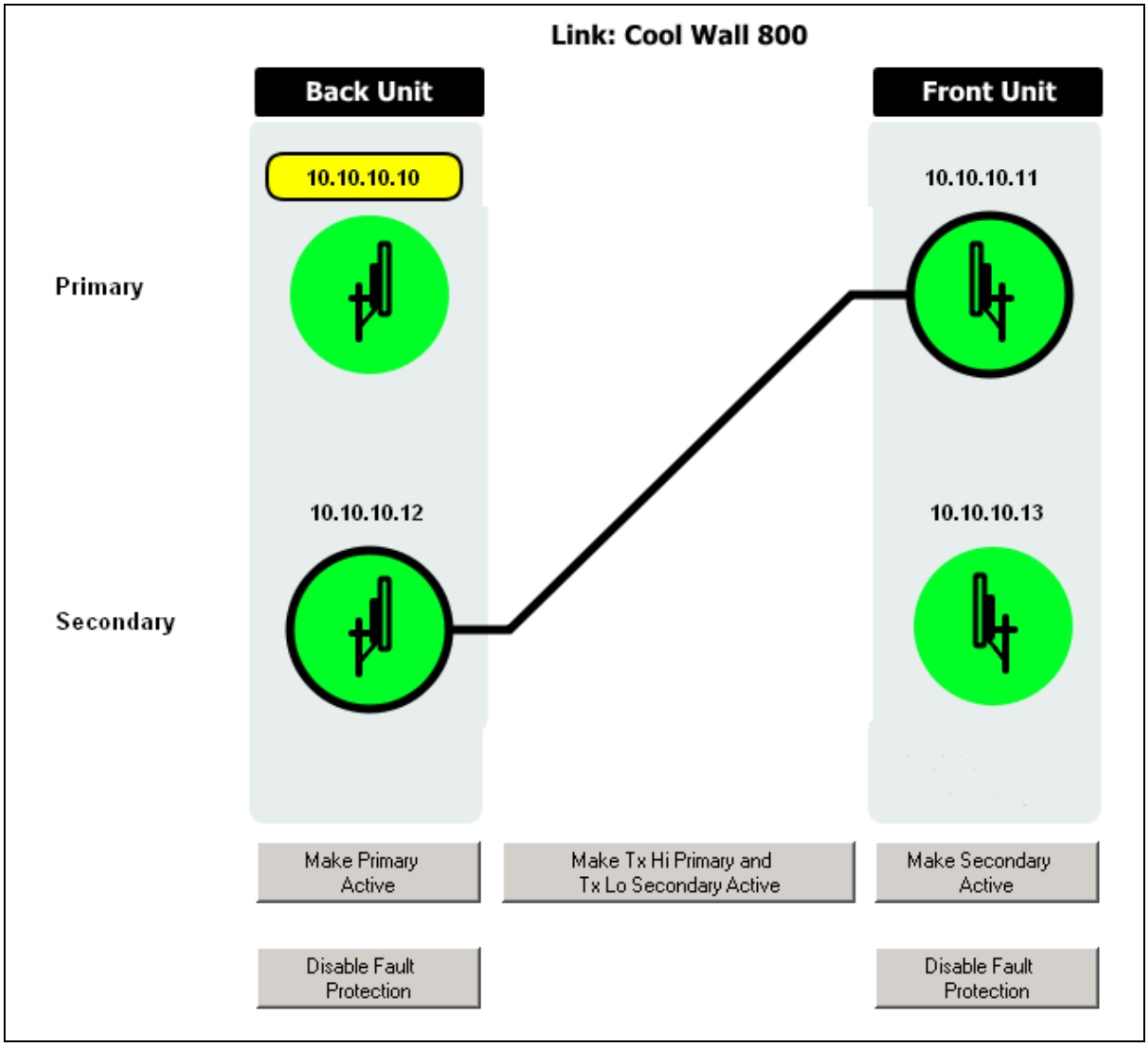
1 Suppose that the initial status is Primary to Primary:



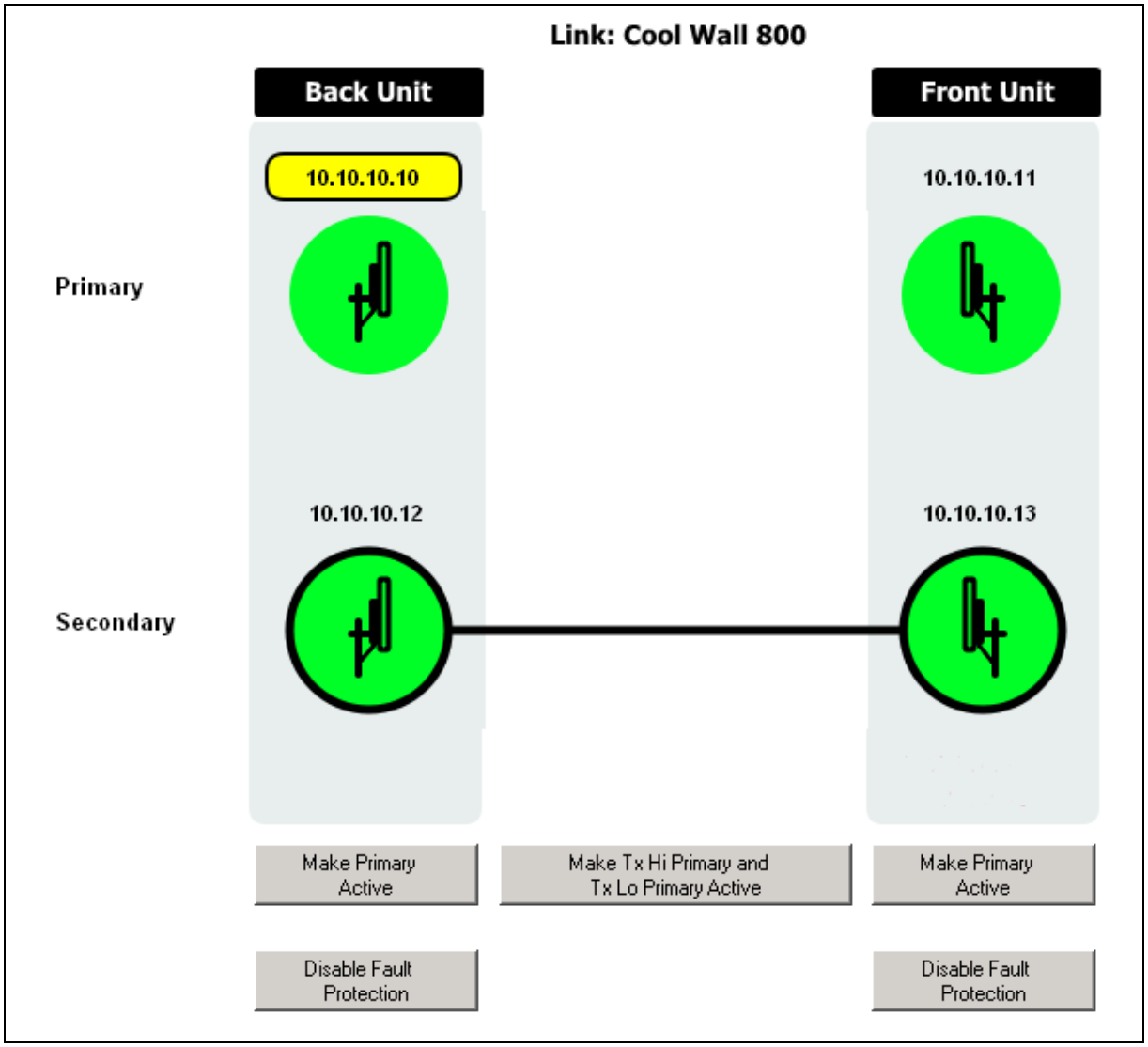
2 Select **Make Secondary Active** at the Tx Lo end. The result is:



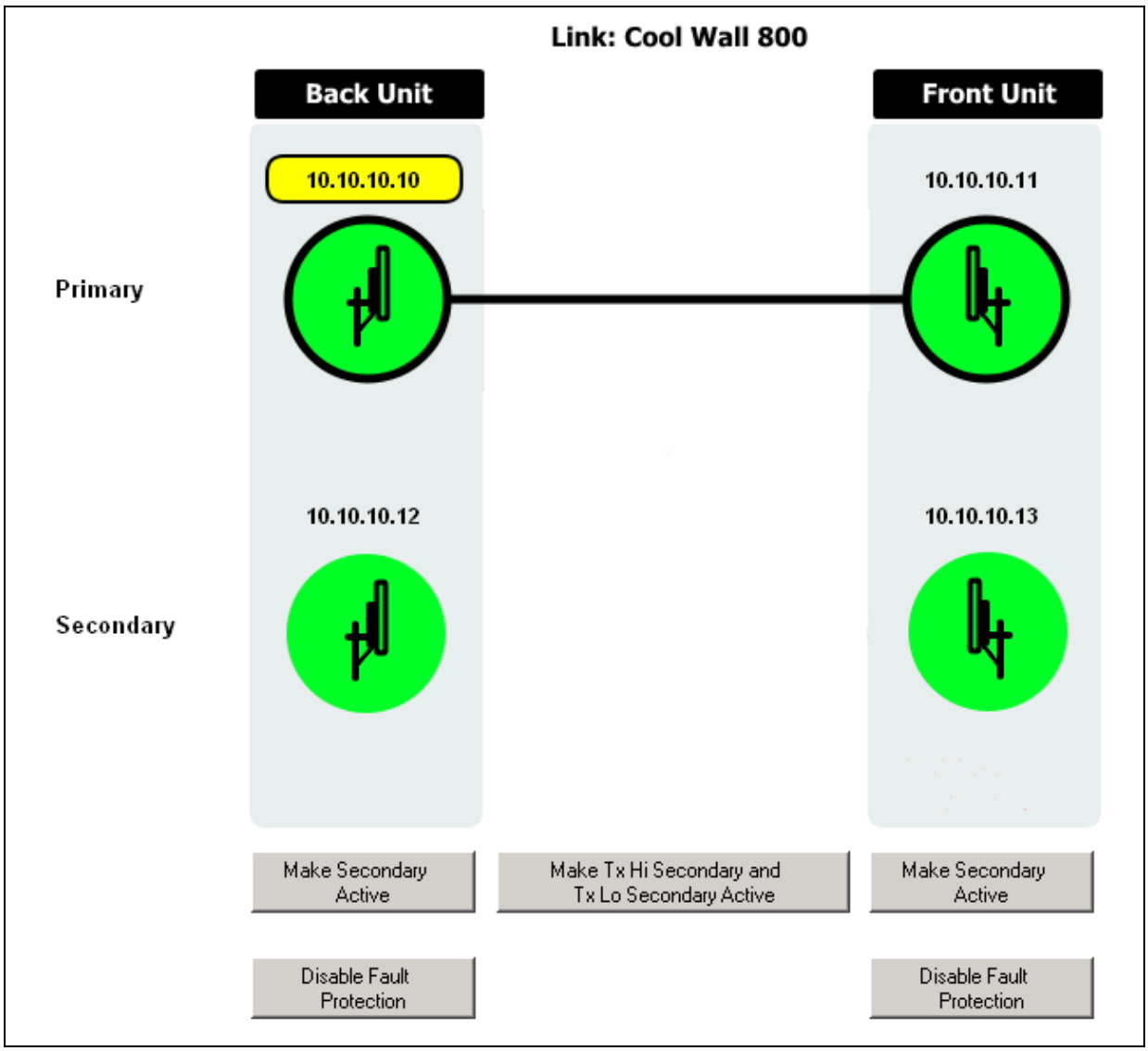
3 Select **Make Tx Hi Secondary and Tx Lo Primary Active**. The result is:



4 Select **Make Secondary Active** at the Tx Lo end. The result is:



5 Select **Make Tx Hi Primary and Tx Lo Primary Active**. The initial status (Primary to Primary) is restored:



Enabling and disabling fault protection

The Protected Link page can be used to enable or disable fault protection switching during the operation of the link. When switching is disabled, a fault will not cause a protection switch, but the user may still manually switch. This feature is intended to be used during maintenance actions where the user does not wish faults to change which CMU/RFU is active.

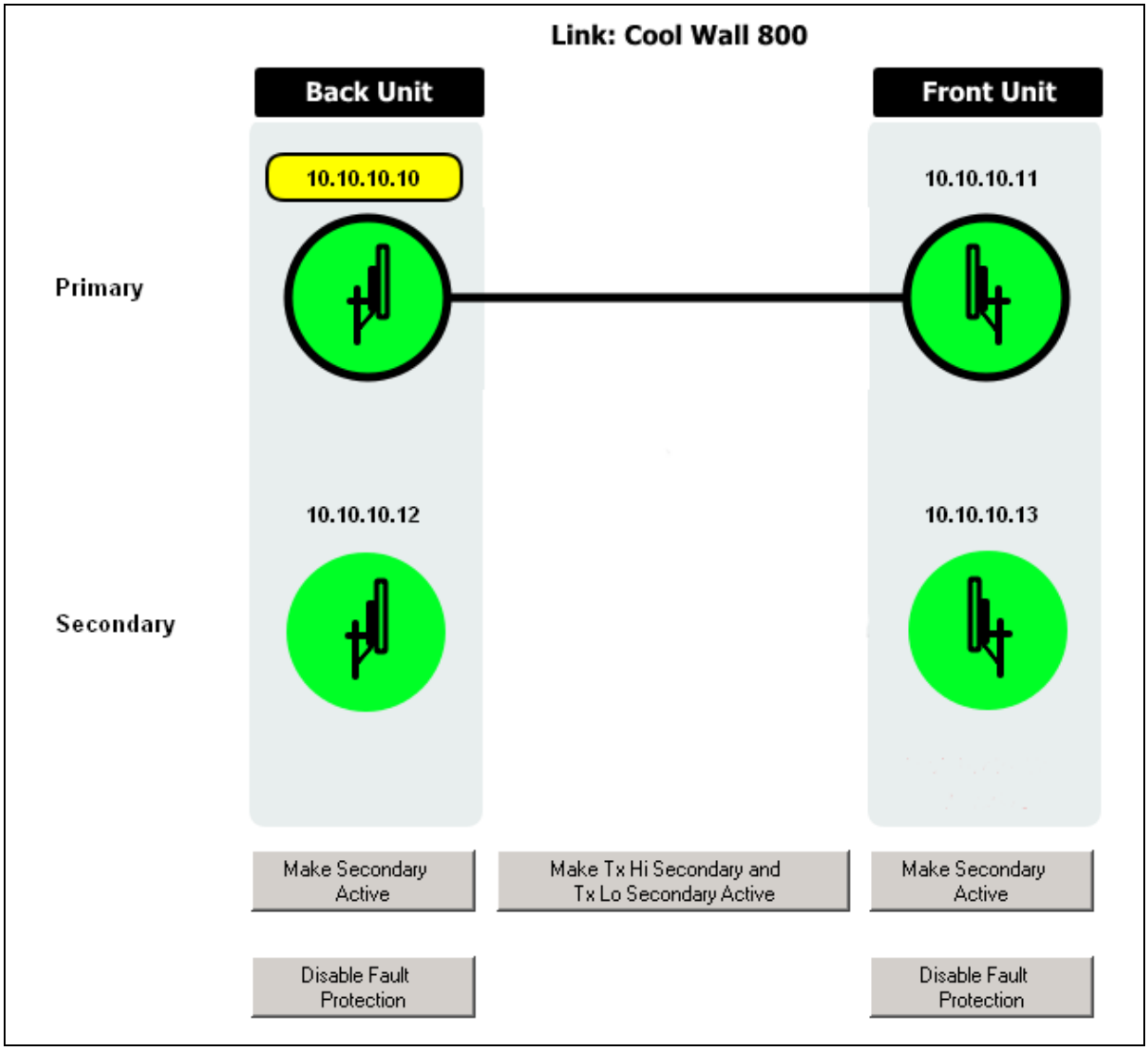
> **NOTE**
> This may be a required state with Spatial Diversity to prevent transmission through a non-compliant diverse antenna.

Enable and disable fault protection using the buttons on the Protected Link page. The text in the buttons varies depending upon which units are active and which are inactive.

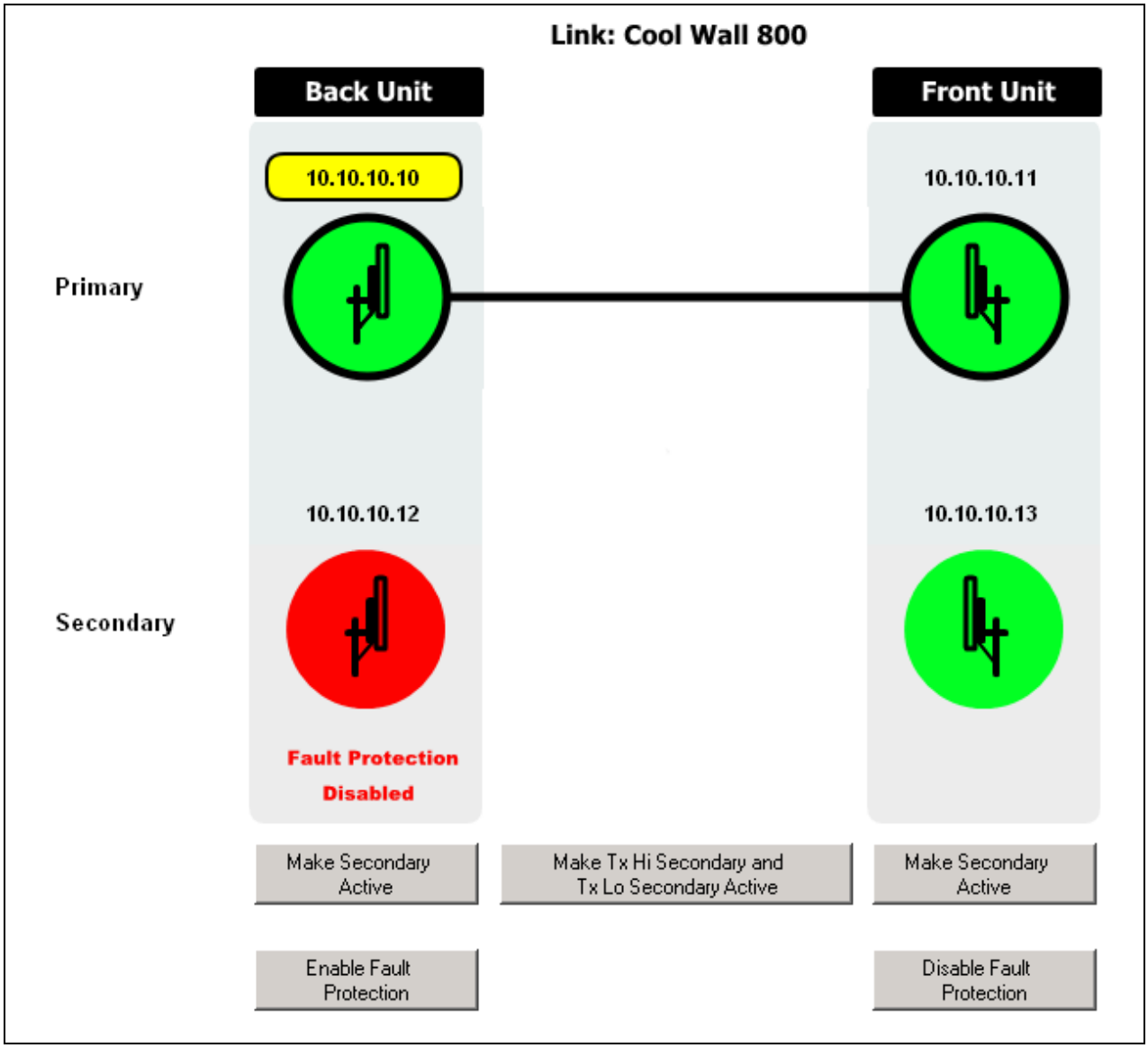
Example

For example, one possible disabling and enabling sequence is as follows:

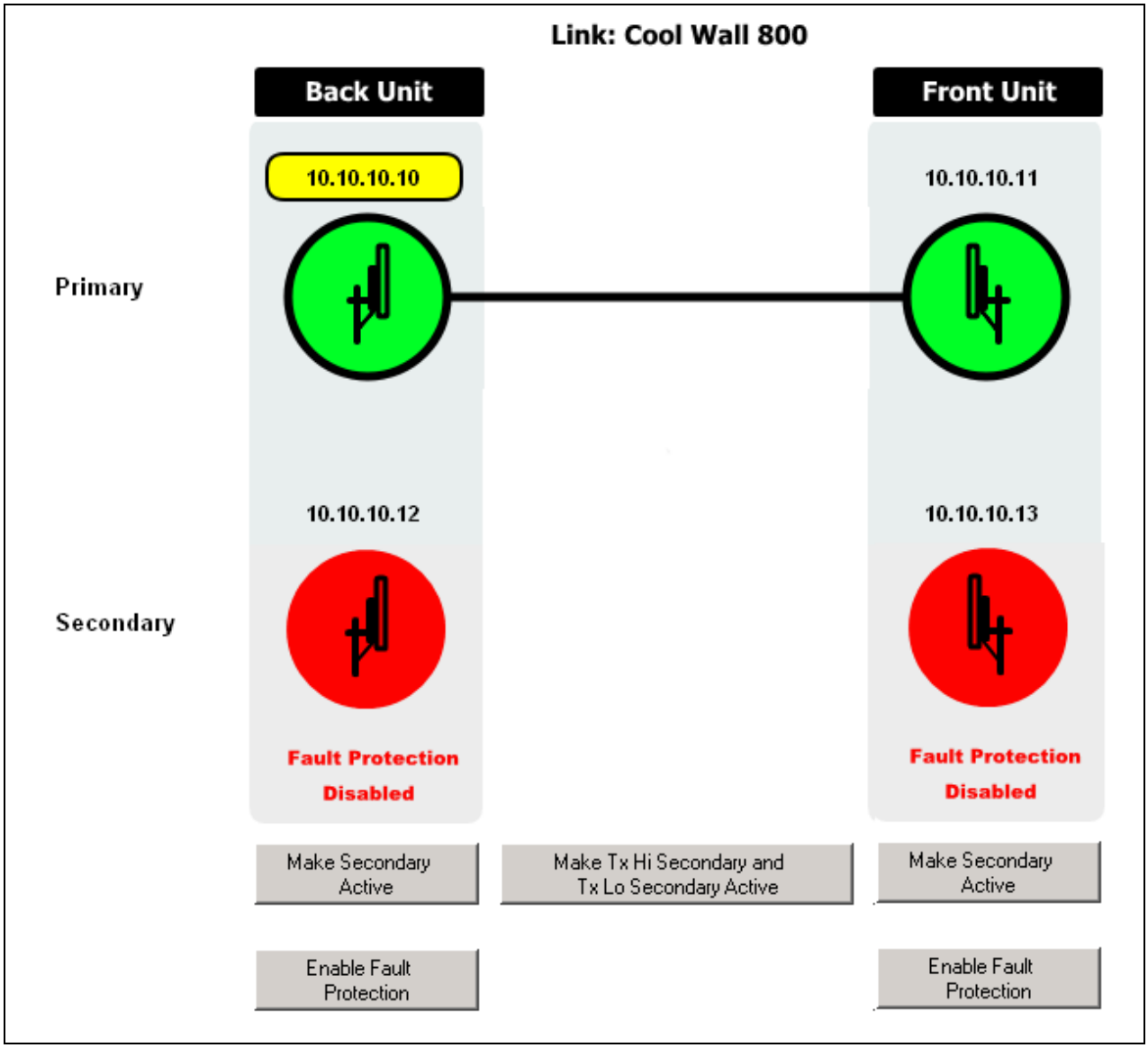
1 Suppose that initially, fault protection is enabled at both ends:



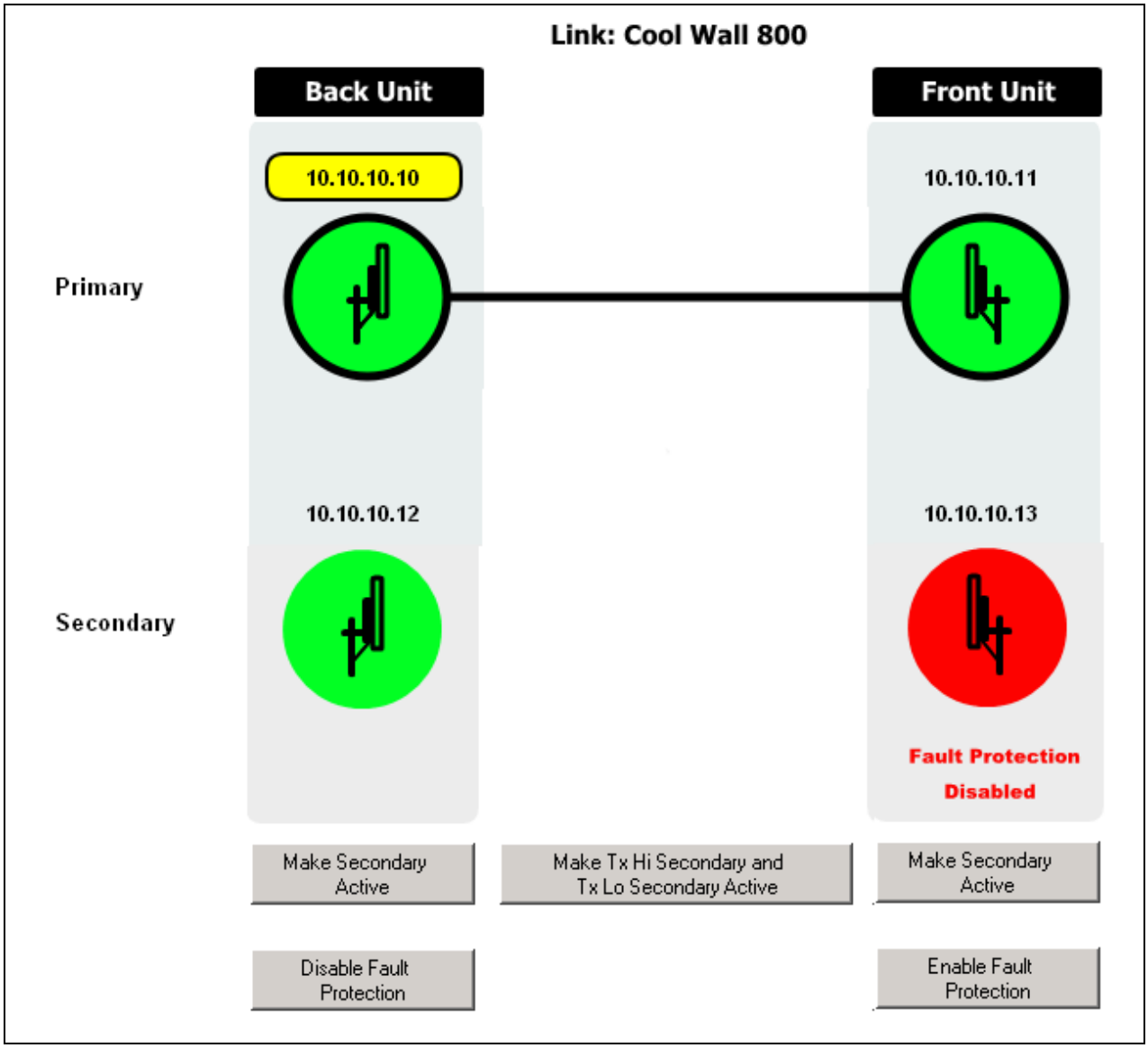
2 Select **Disable Fault Protection** at the Tx Hi end. The result is:



3 Select **Disable Fault Protection** at the Tx Lo end. The result is:



4 Select **Enable Fault Protection** at the Tx Hi end. The result is:



NOTE

Protection switching can also be enabled or disabled from the Protection Configuration page, as described in Task 6: Configuring protection on page 6-53.

Replacing a CMU in a 1+1 Hot Standby link

Pre-configuring the replacement CMU

Before delivering the replacement CMU to the PTP 800 site, ensure that it is ready to operate in the link. Proceed as follows:

1. Connect the replacement CMU to a management PC and open the web interface.
2. Use the latest saved configuration file from the faulty CMU to configure the replacement CMU. For instructions, refer to Restoring the system configuration on page 7-67.

> **NOTE**
> Ensure that the replacement CMU has the same licensed capabilities as the faulty CMU. If necessary, obtain and install a new license key.
>
> If a saved configuration file is not available, use the web interface to configure the replacement CMU as described in Chapter 6: Configuration and alignment.

3. If the installation includes a Fiber-Y interface, select menu option **System, Configuration, Protection** and confirm that Fiber Y is set to 'Enabled'.

> **CAUTION**
> Ensure this is done before replacing the CMU on site. If the Fiber-Y cable is connected to the replacement CMU whilst Fiber-Y is 'Disabled', the Ethernet connection will drop.

4. Select menu option **System, Software Upgrade**. The Software Upgrade page is displayed.
5. Make sure that the application software version is the same as the software installed on the other units in the link.
6. If Fiber-Y is enabled, make sure that:

   Application Software version is 800-04-00 or higher version.

   Boot Software is BOOT-03-00 or higher version.

   Recovery software is RECOVERY-04-00 or higher version

   If the requirements for boot or recovery are not met, contact customer support.

Replacing the CMU on site

To replace the CMU on site, proceed as follows:

1. Identify the faulty CMU. The 1+1 LED state should be orange blink to indicate that the CMU is faulty and not protecting.
2. Remove power cable from the faulty CMU, disconnect all other interface cables, then remove the CMU.
3. Mount the replacement CMU.

> **⚠ CAUTION**
> If the installation includes a Fiber-Y interface, the CMU must have Fiber-Y enabled before executing the remaining steps.

4. Connect interface cables to the replacement CMU (Figure 4), ensuring the power cable is connected last:
   a. Connect IF cable to RFU connector.
   b. If configured for out-of-band management, connect the CMU Management port to the appropriate CMU port of the 1+1 protection splitter.
   c. Connect copper data cable (if used) to copper Data port.
   d. Connect SFP module and fiber cable (if used) to Fiber SFP port.
   e. Connect ground cable to ground stud.
   f. Connect power cable to -48 V DC power socket and power up.
5. After approximately 2 minutes from powering up, check that the Management port 1+1 LED state is either green steady (CMU is active) or green blink (CMU is inactive). If it is in any other state, confirm that the correct CMU has been replaced and re-check the CMU configuration. See Table 5 for details of CMU LED states.

Making the Primary unit the active unit

If the replacement unit is configured as Primary, you may wish to make this the active unit, for example, if it is connected to the lower loss arm of an asymmetric coupler. This can be done by forcing a protection switch, see Managing 1+1 Hot Standby links on page 7-33. Alternatively, the CMU configured as Secondary may be configured with the Primary Recovery feature enabled, in which case there will be an automatic protection switch making the Primary CMU active once the Primary unit has been continually free of faults for a configurable period of time. See Configuring 1+1 Hot Standby links on page 6-54.

Managing security

This section describes how to manage security features such as FIPS 140-2 mode and AES encryption in operational PTP 800 links.

Exiting FIPS 140-2 mode

To exit from the FIPS 140-2 mode, do one of the following:

- Load a PTP 800 license key that has FIPS operation disabled and reboot. Refer to Task 3: Installing license keys on page 6-21.
- Load PTP 800 software that is not FIPS-validated and reboot. Refer to Task 4: Upgrading software version on page 6-25.

> **NOTE**
> The critical security parameters (CSPs) are zeroized when the unit is no longer FIPS 140-2 Capable.

Zeroizing critical security parameters

Critical security parameters (CSPs) are as follows:

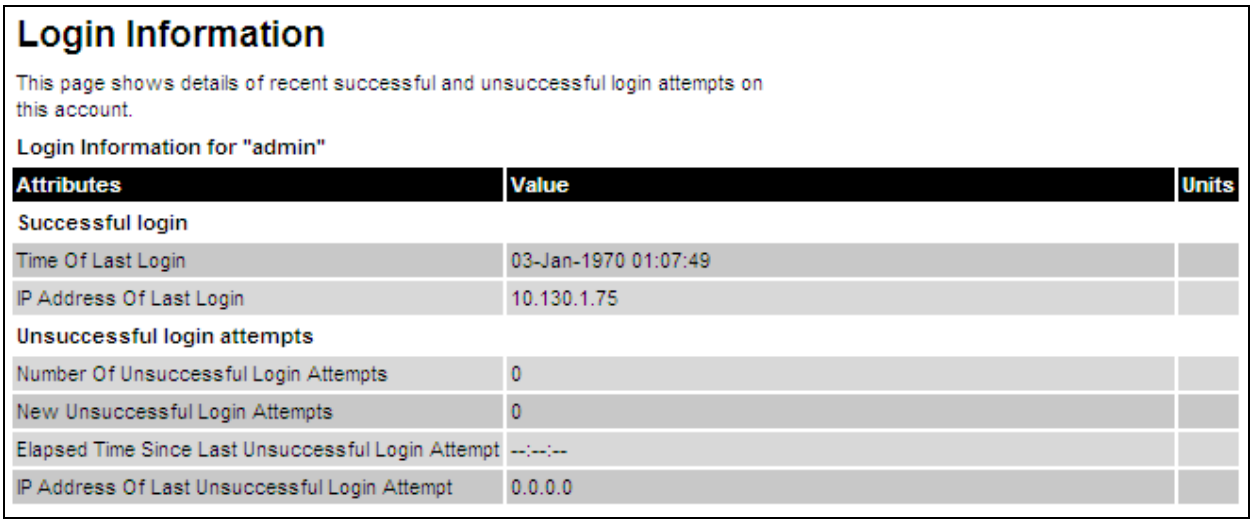
- Key of keys.
- AES encryption keys for the wireless interface.
- Private key for the HTTPS/TLS interface.
- Entropy value for the HTTPS/TLS interface.
- User account passwords for the web-based interface.

To zeroize the CSPs, select option **Security, Zeroize CSPs** and then **Select Zeroize CSPs and Reboot Wireless Unit**. Confirm the reboot. Alternatively, select the **Zeroize CSPs** option in Recovery mode.

Displaying login information

To display details of the most recent successful login, and the most recent unsuccessful login attempt, for each user of the web-based interface, select menu option **Management, Web, Login Information**. The Login Information page is displayed (Figure 191).

Figure 191 Login Information page



Login Information

This page shows details of recent successful and unsuccessful login attempts on this account.

Login Information for "admin"

Attributes	Value	Units
Successful login		
Time Of Last Login	03-Jan-1970 01:07:49	
IP Address Of Last Login	10.130.1.75	
Unsuccessful login attempts		
Number Of Unsuccessful Login Attempts	0	
New Unsuccessful Login Attempts	0	
Elapsed Time Since Last Unsuccessful Login Attempt	--:--:--	
IP Address Of Last Unsuccessful Login Attempt	0.0.0.0	

Disabling AES encryption

Perform this task to disable the encryption of data transmitted over the PTP 800 bridge. For more information on AES encryption, see AES license on page 1-60

This procedure must be repeated at both ends of the link.

⚠ CAUTION

If AES encryption is disabled at one end of the link, it must also be disabled at the other end of the link, otherwise the link will not work.

Unprotected link

To disable AES encryption for an unprotected link, proceed as follows:

1. Select menu option **Configuration**. The System Configuration page is displayed (Figure 172).
2. Set the Encryption Algorithm attribute to ‘None’.
3. Select **Submit Updated System Configuration**. The Configuration Change Reboot dialog is displayed.

4 Select **Reboot Wireless Unit**. The Reboot Confirmation dialog is displayed.

5 Select **OK**. The reboot progress message is displayed. On completion, the unit restarts with AES encryption disabled.

1+1 Hot Standby link

To disable AES encryption for a 1+1 Hot Standby link, proceed as follows:

1 If link planning indicates that the inactive units are not able to operate a link of satisfactory quality, force a protection switch at one end of the wireless link.

2 Disable fault protection switching for all PTP 800 units, as described in Enabling and disabling fault protection on page 7-43.

3 Disable AES Encryption for both inactive PTP 800 units as defined above for unprotected links.

4 Force a simultaneous protection switch at both ends of the wireless link, as described in Forcing protection switches on page 7-37. Check that the link is operating correctly without encryption.

5 Disable AES Encryption for both newly inactive PTP 800 units as defined in the above procedure for unprotected links.

6 Force a simultaneous protection switch at both ends of the wireless link, as described in Forcing protection switches on page 7-37. Check that the link is operating correctly without encryption.

7 If a protection switch was forced at one end of the link (Step 1) force a protection switch at the other end of the link so that the link is operated by the two primary units.

8 Re-enable protection switching for all PTP 800 units, as described in Enabling and disabling fault protection on page 7-43.

Changing AES encryption keys

Perform this task to update the encryption key used for data transmitted over the PTP 800 bridge. For more information on AES encryption, see AES license on page 1-60

This procedure must be repeated at both ends of the link.

⚠ CAUTION

If the AES encryption key is changed at one end of the link, it must also be changed to the same value at the other end of the link, otherwise the link will not work.

Unprotected link

To change the AES encryption key for an unprotected link, proceed as follows:

1. Select menu option **Configuration**. The System Configuration page is displayed (Figure 172).
2. If the encryption attributes are not displayed, or if the Encryption Key attribute is set to 'None', see Configuring AES encryption on page 6-29.
3. Update the Encryption Key attribute.
4. Select **Submit Updated System Configuration**. The Configuration Change Reboot dialog is displayed.
5. Select **Reboot Wireless Unit**. The Reboot Confirmation dialog is displayed.
6. Select **OK**. The reboot progress message is displayed. On completion, the unit restarts with AES encryption enabled, using the new key.

1+1 Hot Standby link

This procedure must be performed for all units. When upgrading each pair of units, then either the web interface can be opened simultaneously for each CMU, or the remote system can be configured and then the local system configured.

NOTE

Before changing encryption keys, check that no alarms are outstanding for the units to be upgraded. See Managing alarms on page 7-15.

It is expected that this procedure will normally take place from an initial status of Primary to Primary, especially for an asymmetric coupler or for a protected antenna when the inactive unit has a lower capacity.

To change the AES encryption key for a 1+1 Hot Standby link, proceed as follows:

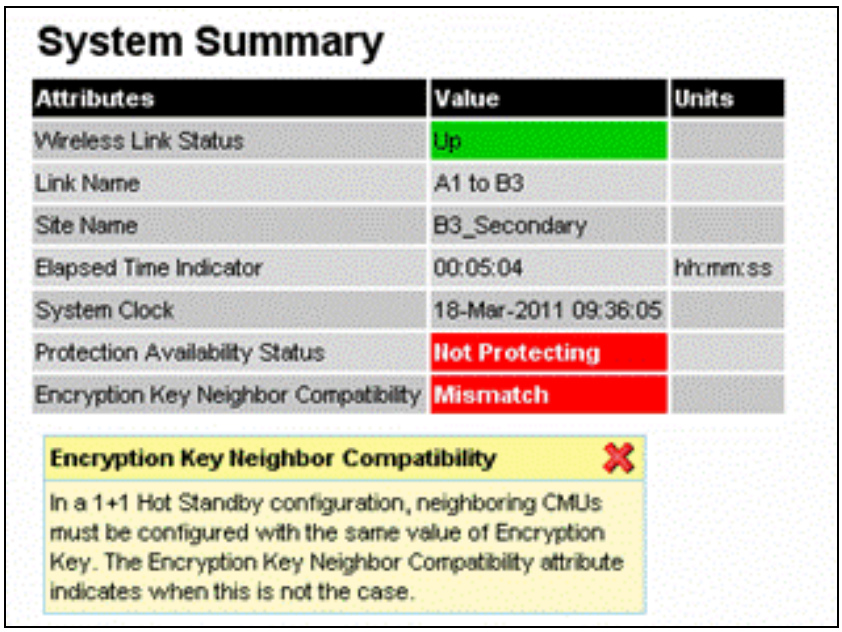
1. Disable local and remote protection switching, as described in Enabling and disabling fault protection on page 7-43.
2. Force a protection switch at the local end of the wireless link, as described in Forcing protection switches on page 7-37, so that the link is operating between a primary and a secondary unit.
3. Change AES Encryption keys for both inactive PTP 800 units, as defined in Unprotected link on page 7-54.

CAUTION

If an incorrect encryption key is entered at the remote end, then it may be necessary to go to the remote end to correct the encryption key.

4. Force a simultaneous protection switch at both ends of the wireless link, as described in Forcing protection switches on page 7-37. Check that the link is operating correctly using the new encryption key.
5. Change AES Encryption keys for both newly inactive PTP 800 units, as defined in Unprotected link on page 7-54.
6. Check the System Status page for encryption alarms (Figure 192). If any are displayed, investigate and correct the encryption configuration.
7. Force a simultaneous protection switch at both ends of the wireless link, as described in Forcing protection switches on page 7-37. Check that the link is operating correctly using the new encryption keys.
8. Force a protection switch at the local end of the link, so that the link is running Primary to Primary, and check that the link is operating correctly. This confirms that the new encryption key is the same for all four units.
9. Re-enable local and remote protection switching, as described in Enabling and disabling fault protection on page 7-43.

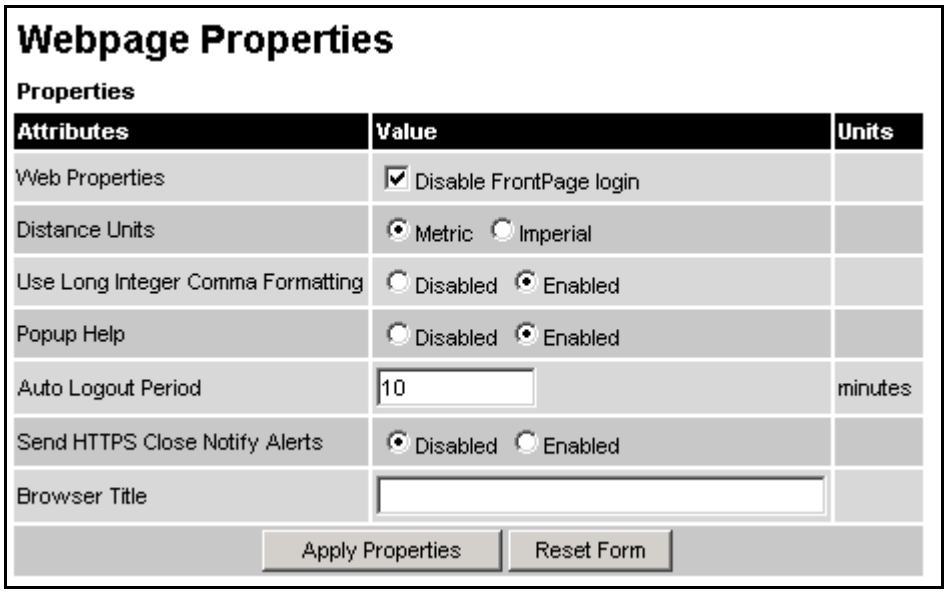
Figure 192 Encryption key mismatch



Changing the log-out timer

The automatic logout time period is the amount of time without user activity that is allowed to elapse before the system administrator is logged off. To change the log-out timer, select menu option **Properties**. The Web Page Properties page is displayed (Figure 193). Set the Auto Logout Timer attribute to the number of minutes that should elapse before automatic logout occurs. If automatic logout is not wanted, set Auto Logout Timer to zero. This means that the system administrator will remain logged on, with or without user activity. Select **Apply Properties**.

Figure 193 Web Page Properties page



Managing performance

This section describes how to view and manage PTP 800 system statistics and diagnostics.

Checking system statistics and counters

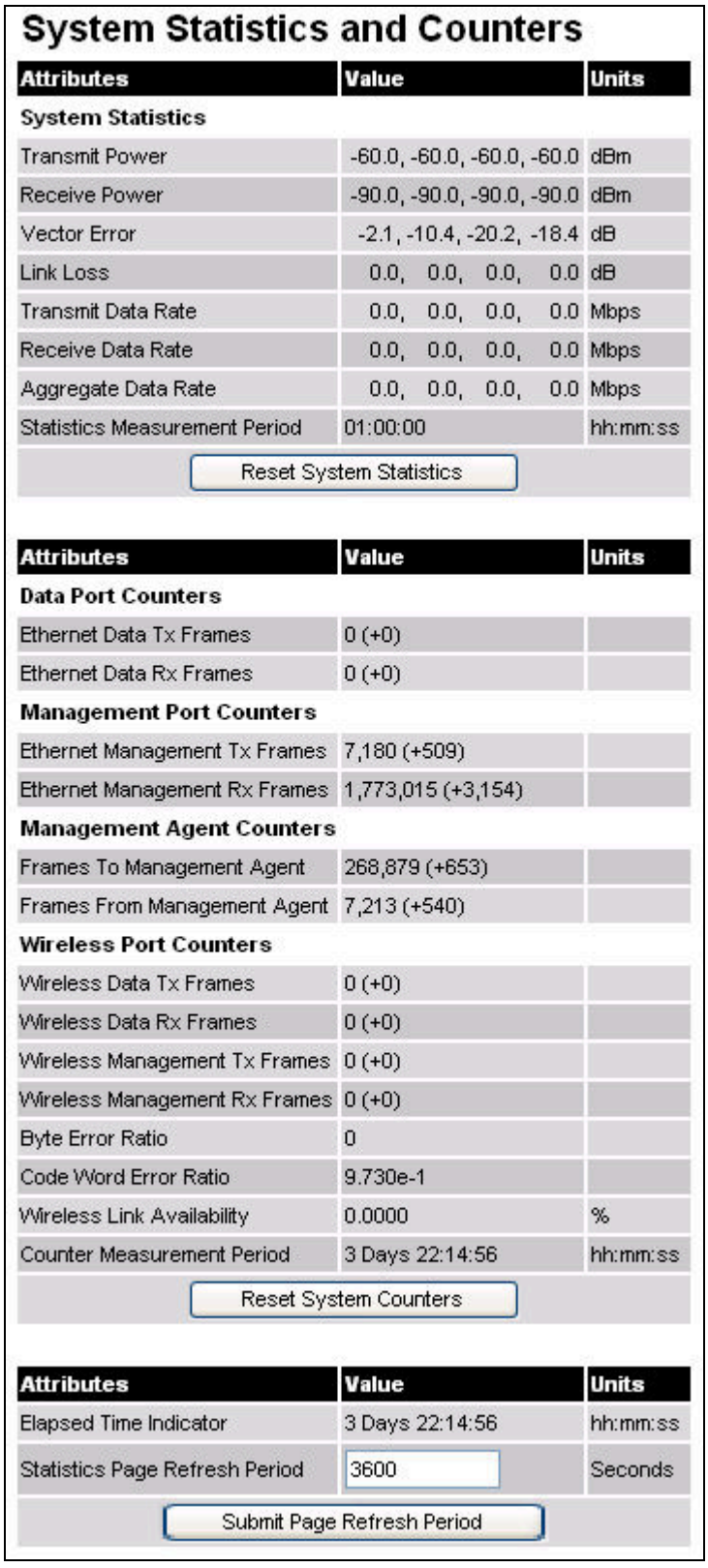
To check system statistics and counters, select menu option **Statistics**. The System Statistics and Counters page is displayed (Figure 194). Review the statistics and counters (Table 261).

> **NOTE**
> To enable or disable the display of commas in long integers (for example 1,234,567), select **Properties** from the menu and update the Use Long Integer Comma Formatting attribute.

> **NOTE**
> Transmit power, receive power, vector error and link loss are presented as an array of four elements. These elements represent the maximum, mean, minimum and latest values respectively. The maximum, mean and minimum are calculated over a running one hour period.

> **NOTE**
> The frame counter attributes each contain a number in parentheses; this shows the number of frames received since the last page refresh.

Figure 194 System Statistics and Counters page



System Statistics and Counters

Attributes	Value	Units
System Statistics		
Transmit Power	-60.0, -60.0, -60.0, -60.0	dBm
Receive Power	-90.0, -90.0, -90.0, -90.0	dBm
Vector Error	-2.1, -10.4, -20.2, -18.4	dB
Link Loss	0.0, 0.0, 0.0, 0.0	dB
Transmit Data Rate	0.0, 0.0, 0.0, 0.0	Mbps
Receive Data Rate	0.0, 0.0, 0.0, 0.0	Mbps
Aggregate Data Rate	0.0, 0.0, 0.0, 0.0	Mbps
Statistics Measurement Period	01:00:00	hh:mm:ss

Reset System Statistics

Attributes	Value	Units
Data Port Counters		
Ethernet Data Tx Frames	0 (+0)	
Ethernet Data Rx Frames	0 (+0)	
Management Port Counters		
Ethernet Management Tx Frames	7,180 (+509)	
Ethernet Management Rx Frames	1,773,015 (+3,154)	
Management Agent Counters		
Frames To Management Agent	268,879 (+653)	
Frames From Management Agent	7,213 (+540)	
Wireless Port Counters		
Wireless Data Tx Frames	0 (+0)	
Wireless Data Rx Frames	0 (+0)	
Wireless Management Tx Frames	0 (+0)	
Wireless Management Rx Frames	0 (+0)	
Byte Error Ratio	0	
Code Word Error Ratio	9.730e-1	
Wireless Link Availability	0.0000	%
Counter Measurement Period	3 Days 22:14:56	hh:mm:ss

Reset System Counters

Attributes	Value	Units
Elapsed Time Indicator	3 Days 22:14:56	hh:mm:ss
Statistics Page Refresh Period	3600	Seconds

Submit Page Refresh Period

Table 261 System Statistics and Counters attributes

Attribute	Meaning
System Statistics	
Transmit Power	The maximum, mean, minimum and latest measurements of Transmit Power.
Receive Power	The maximum, mean, minimum and latest measurements of Receive Power.
Vector Error	The maximum, mean, minimum and latest measurements of Vector Error. Normalized Mean Square Vector Error is a measure of quality for the received signal after all corrections made by the demodulator. The value is generally in the range from -3 dB to -35 dB. A more negative number indicates a higher quality signal.
Link Loss	The maximum, mean, minimum and latest measurements of Link Loss. Link Loss is a measurement of the loss in signal level as the radio wave propagates between the antennas installed at each end of the link. It is determined by measurement of the receive level, the transmit power of the remote end and the antenna gains and feeder losses at each end of the link. The Link Loss is therefore only accurate if the correct antenna gains and feeder losses have been configured at both ends of the link. Link Loss (dB) = Remote Transmit Power (dBm) - Remote Feeder Loss (dB) + Remote Antenna Gain (dBi) + Local Antenna Gain (dBi) - Local Feeder Loss (dB) - Local Receive Power (dBm).
Transmit Data Rate	The data rate in the transmit direction, expressed in Mbps and presented as: max, mean, min, and latest in an histogram format. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means.
Receive Data Rate	The data rate in the receive direction, expressed in Mbps and presented as: max, mean, min, and latest in an histogram format. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means.

Attribute	Meaning
Aggregate Data Rate	The sum of the data rate in the directions expressed in Mbps and presented as: max, mean, min, and latest in an histogram format. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means.
Statistics Measurement Period	The time over which the system statistics were collected.
Data Port Counters	
Ethernet Data Tx Frames	Count of Ethernet frames transmitted at the data port.
Ethernet Data Rx Frames	Count of Ethernet frames received at the data port.
Management Port Counters	
Ethernet Management Tx Frames	Count of Ethernet frames transmitted at the management port.
Ethernet Management Rx Frames	Count of valid Ethernet frames received at the management port.
Management Agent Counters	
Frames To Management Agent	Count of Ethernet frames processed by the management agent.
Frames From Management Agent	Count of Ethernet frames generated by the management agent.
Wireless Port Counters	
Wireless Data Tx Frames	Count of Ethernet frames transmitted at the data channel of the wireless port.
Wireless Data Rx Frames	Count of Ethernet frames received at the data channel of the wireless port.
Wireless Management Tx Frames	Count of Ethernet frames transmitted at the management channel of the wireless port.
Wireless Management Rx Frames	Count of Ethernet frames received at the management channel of the wireless port.
Byte Error Ratio	Byte error ratio calculated since the last reset of the system counters.

Attribute	Meaning
Code Word Error Ratio	Code Word Error Ratio provides an indication of wireless link performance in the direction towards the unit where the attribute is being monitored. Data transmitted over the wireless link is organized into blocks called Code Words. The size of the code word is fixed for a given configuration of bandwidth. The transmitter applies Forward Error Correction (FEC) to each Code Word and this allows the receiver to correct certain Code Words which have been received in error. If the receiver cannot correct a Code Word, it will be counted as a Code Word Error. This may occur if the link fades below the sensitivity threshold of the minimum modulation. The Code Word Error Ratio is the ratio of Code Words Errors to the total number of Code Words received, calculated since the last reset of the system counters.
Wireless Link Availability	Link availability calculated since the last reset of the system counters.
Protection (Detailed counters)	
Active Elapsed Time	This is the time that the CMU/RFU has been in the active role of a 1+1 Hot Standby configuration since the last statistics reset.
Active Available Time	This is the time which the Wireless link status has been up whilst the CMU/RFU has been in the Active role of a 1+1 Hot Standby configuration. The reported time is since the last statistics reset.
Active Byte Count	This reports the number of bytes received over the wireless interface whilst the CMU/RFU is in the Active role of a 1+1 Hot Standby configuration. This count is since the last statistics reset.
Active Byte Error Count	This reports the number of byte errors which have been detected over the wireless interface whilst the CMU/RFU is in the Active role of a 1+1 Hot Standby configuration. This count is since the last statistics reset.
Other attributes	
Elapsed Time Indicator	Time elapsed since the last system reboot.
Statistics Page Refresh Period	Automatic page refresh period in seconds.

Resetting system statistics and counters

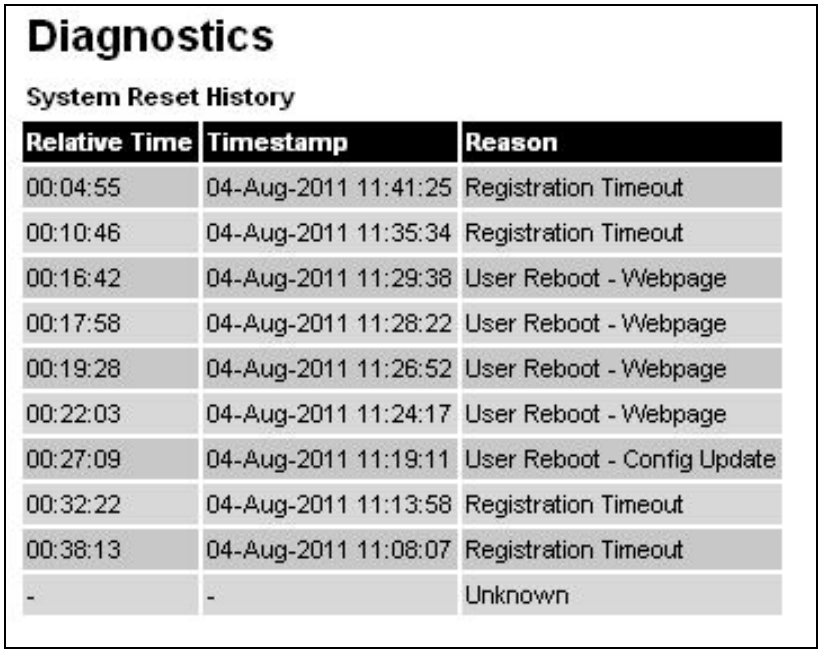
To check system statistics and counters, select menu option **Statistics**. The System Statistics and Counters page is displayed (Figure 194). To reset the System Statistics attributes, select **Reset System Statistics**. To reset the Counters attributes, select **Reset System Counters**.

Viewing diagnostics

To view the Diagnostics page, select menu option **System, Diagnostics**.

In 1+0 or 2+0 links, the Diagnostics page displays a history of previous system resets (Figure 195). In 1+1 Hot Standby links, it displays the reset history and also a history of protection switches (Figure 196).

Figure 195 Diagnostics page (1+0 or 2+0 link)



Diagnostics

System Reset History

Relative Time	Timestamp	Reason
00:04:55	04-Aug-2011 11:41:25	Registration Timeout
00:10:46	04-Aug-2011 11:35:34	Registration Timeout
00:16:42	04-Aug-2011 11:29:38	User Reboot - Webpage
00:17:58	04-Aug-2011 11:28:22	User Reboot - Webpage
00:19:28	04-Aug-2011 11:26:52	User Reboot - Webpage
00:22:03	04-Aug-2011 11:24:17	User Reboot - Webpage
00:27:09	04-Aug-2011 11:19:11	User Reboot - Config Update
00:32:22	04-Aug-2011 11:13:58	Registration Timeout
00:38:13	04-Aug-2011 11:08:07	Registration Timeout
-	-	Unknown

Figure 196 Diagnostics page (1+1 link)



Diagnostics

System Reset History

Relative Time	Timestamp	Reason
00:03:47	04-Aug-2011 11:41:25	Registration Timeout
00:09:38	04-Aug-2011 11:35:34	Registration Timeout
00:15:34	04-Aug-2011 11:29:38	User Reboot - Webpage
00:16:50	04-Aug-2011 11:28:22	User Reboot - Webpage
00:18:20	04-Aug-2011 11:26:52	User Reboot - Webpage
00:20:55	04-Aug-2011 11:24:17	User Reboot - Webpage
00:26:01	04-Aug-2011 11:19:11	User Reboot - Config Update
00:31:14	04-Aug-2011 11:13:58	Registration Timeout
00:37:05	04-Aug-2011 11:08:07	Registration Timeout
-	-	Unknown

Protection Switch History

Relative Time	Timestamp	Reason
01:16:11	04-Aug-2011 10:29:01	Managed Protection Switch
01:16:25	04-Aug-2011 10:28:47	Data Port Down
01:17:06	04-Aug-2011 10:28:06	Managed Protection Switch
01:17:41	04-Aug-2011 10:27:31	Wireless Receive Signal Not Detected at Remote End
01:18:34	04-Aug-2011 10:26:38	Managed Protection Switch
01:18:58	04-Aug-2011 10:26:14	ODU Tx Synth Out of Lock
01:19:12	04-Aug-2011 10:26:00	Managed Protection Switch
01:19:27	04-Aug-2011 10:25:45	ODU Rx Synth Out of Lock
01:19:53	04-Aug-2011 10:25:19	Managed Protection Switch
01:20:17	04-Aug-2011 10:24:55	ODU Not Responding

Using the diagnostics plotter

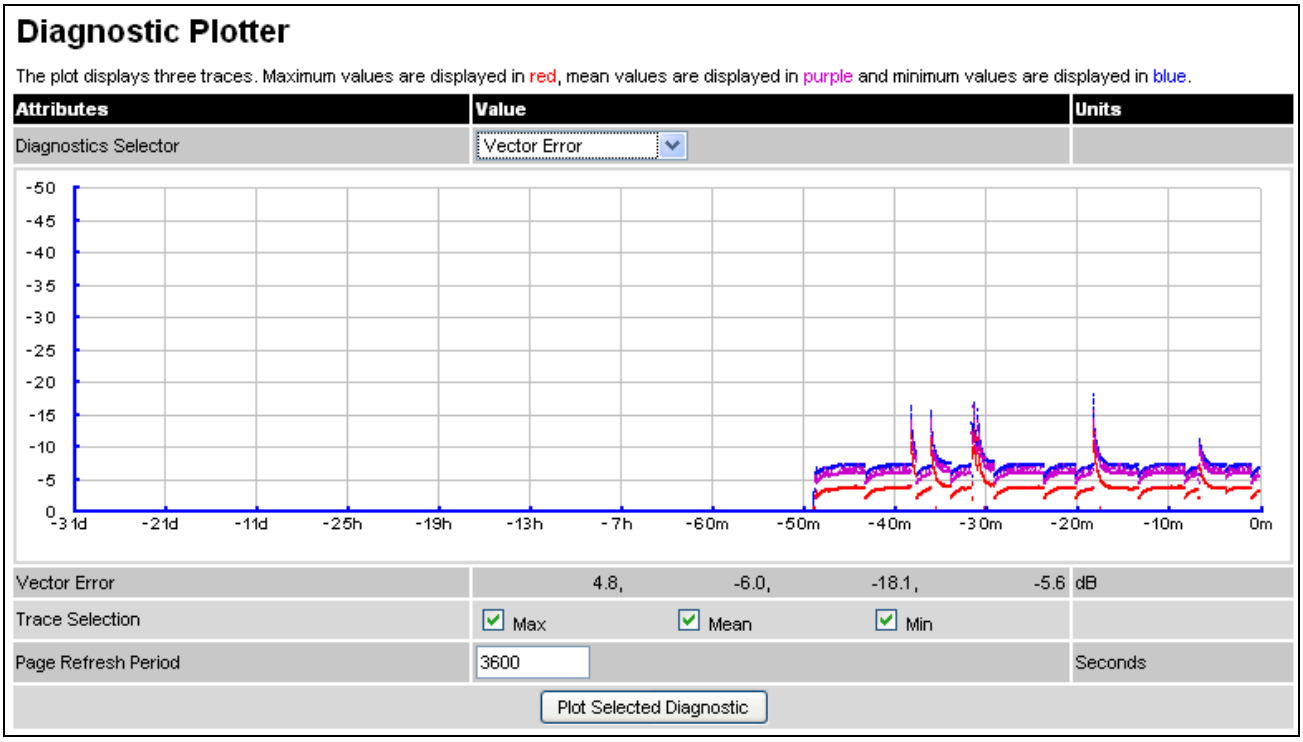
The diagnostics plotter can trace the following statistics (refer to Table 261 for definitions):

- Vector Error
- Rx Power
- Tx Power
- Link Loss
- Rx Data Rate
- Tx Data Rate
- Aggregate Data Rate
- Protection State: In a 1+1 Hot Standby configuration, only one CMU / RFU at a given end of the link is Active at any one time, the neighbor CMU / RFU being Inactive. The Protection State indicates whether a CMU / RFU is in the Active or Inactive state.
- Remote Primary Secondary Mode: This indicates the Primary /Secondary Mode of the active unit at the remote end of the wireless link.

To plot diagnostics, proceed as follows:

1. Select menu option **System, Diagnostics,** Diagnostics Plotter. The Diagnostics Plotter page is displayed (Figure 197).
2. Use the Diagnostics Selector drop-down list to select a diagnostic type to plot.
3. Use the Trace Selection to select traces of the maximum, mean or minimum values of the diagnostic type. Maximum values are displayed in red, mean values are displayed in purple and minimum values are displayed in blue.
4. Select **Plot Selected Diagnostic**. The trace is displayed in the graph.

Figure 197 Diagnostics Plotter page



Downloading diagnostic data

Perform this task to download snapshots of the system diagnostics to a CSV file.

The CSV file contains at most 5784 entries, recorded over a 32 day period:

- 3600 entries recorded in the last hour.
- 1440 entries recorded in the previous 24 hours.
- 744 entries recorded in the previous 31 days.

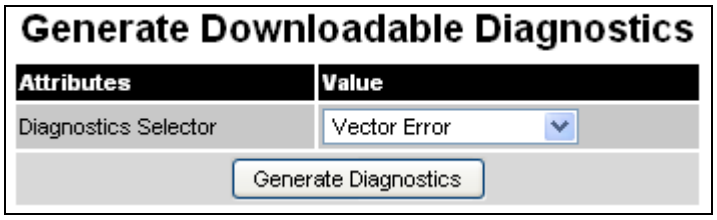
The following statistics can be downloaded (refer to Table 261 for definitions):

- Vector Error
- Rx Power
- Tx Power
- Link Loss
- Rx Data Rate
- Tx Data Rate
- Aggregate Data Rate
- Protection State
- Remote Primary Secondary Mode

To download diagnostics data, proceed as follows:

1. Select menu option **CSV Download**. The Generate Downloadable Diagnostics page is displayed (Figure 198).
2. Use the Diagnostics Selector drop-down list to select a diagnostic type to download.
3. Select **Generate Diagnostics**. The Generate Downloadable Diagnostics page is redisplayed with the name of the generated CSV file.
4. Click on the CSV file name and select **Save File**. Save the CSV file to the hard drive of the local computer.
5. Open the CSV file in MS Excel and use it to generate statistical reports and diagrams.

Figure 198 Generate Downloadable Diagnostics page



Changing the diagnostics refresh period

The default refresh period is 3600 seconds (1 hour). If a much shorter refresh period is selected, for example 60 seconds, it is possible to monitor the performance of an operational PTP 800 link in real time. To change the diagnostics refresh period, select menu option **Diagnostics Plotter**. The Diagnostics Plotter page is displayed (Figure 197). Enter the required refresh frequency in the Page Refresh Period attribute.

Maintaining the system

Once installed, a PTP 800 link should require little or no maintenance.

Yearly maintenance

Recommended yearly physical maintenance:

- Check cables for corrosion, chafing etc.
- Check waterproofing.
- Check ground points for corrosion, tightness etc.

Monthly maintenance

Recommended monthly radio maintenance:

- Read Link Loss and compare against last reading.
- Read ByteER and compare against last reading.

1+1 Hot Standby link maintenance

For a 1+1 Hot Standby link, consider a controlled switchover to the inactive unit (once every three months), to confirm that it is fully functional.

NOTE

This can cause a short interruption to traffic and should be scheduled accordingly to minimize the effects.

Restoring, upgrading and rebooting

This section describes how to restore the system configuration, upgrade the software and reboot the unit.

This section contains the following procedures:

- Restoring the system configuration on page 7-67
- Upgrading software on page 7-68
- Rebooting on page 7-69
- Upgrading software in an operational 1+1 Hot Standby link on page 7-69
- Checking the recovery version on page 7-70

Restoring the system configuration

Perform this procedure to restore a PTP 800 CMU to a previously saved configuration. Refer to Saving the system configuration on page 6-119 for instructions on when and how to save the configuration.

> **NOTE**
> The restore is only guaranteed to work if the installed software version has not been changed since the configuration file was saved. This is why the configuration should always be saved immediately after upgrading the software version.

Licensed capabilities

The license key is restored automatically if the configuration file is saved and then loaded on the same unit. However, the license key is not restored if the configuration file is loaded on a different unit. Before restoring configuration to a different PTP 800 unit, ensure that a valid license key is installed (with optional capabilities enabled where appropriate). For instructions, see Task 3: Installing license keys on page 6-21.

Restoring from the configuration file

To restore the system configuration from file, select menu option **Configuration, Save And Restore**. The Save & Restore Configuration page is displayed (Figure 177). Select **Browse** and navigate to the PC folder containing the saved configuration file (.cfg). Select **Restore Configuration File and Reboot**. Select **OK** to confirm the restore. The configuration file is uploaded and used to reconfigure the new unit to the same state as the old unit. On completion, the unit reboots.

Attributes excluded from save and restore

Most of the configuration can be restored from the backup. However, certain attributes that were part of the configuration are not saved or restored automatically. Use the web interface to reconfigure the following attributes:

- Usernames, passwords and roles for the web-based interface.
- Password complexity controls
- Key of Keys
- HTTPS Entropy
- HTTPS Private Key
- HTTPS Public Key Certificate
- HTTP Access Enabled
- HTTPS Access Enabled
- Telnet Access Enabled
- HTTP Port Number
- HTTPS Port Number
- Telnet Port Number
- Encryption Algorithm
- Encryption Key
- SNMP Control Of HTTP And Telnet

Upgrading software

For instructions on how to check the installed software version and upgrade to a new version, see Task 4: Upgrading software version on page 6-25.

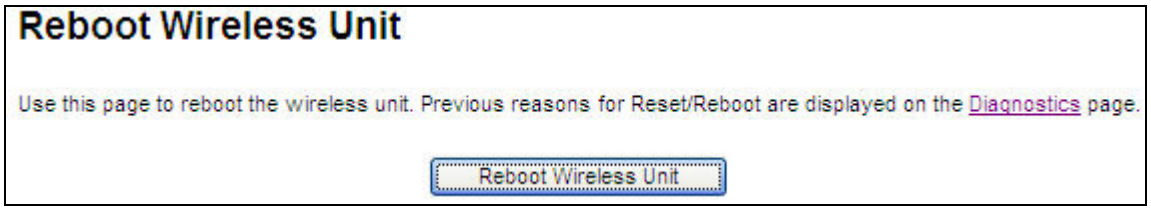
Rebooting

To reboot the CMU, select menu option **Reboot**. The Reboot Wireless Unit page is displayed (Figure 199). Select **Reboot Wireless Unit**. The Reboot Confirmation dialog is displayed. Select **OK**. The reboot progress message is displayed. On completion, the unit restarts.

NOTE

Use the Diagnostics page to view previous rebbot reasons (see Viewing diagnostics on page 7-62).

Figure 199 Reboot Wireless Unit page


Reboot Wireless Unit
Use this page to reboot the wireless unit. Previous reasons for Reset/Reboot are displayed on the Diagnostics page.
Reboot Wireless Unit

Upgrading software in an operational 1+1 Hot Standby link

In 1+1 Hot Standby links, the forced protection switch minimizes the link down time, since all units are inactive when upgraded. Protection switching to the newly upgraded units allows a fallback path should the upgrade have problems.

CAUTION

Upgrading in a different order could make the remote end of the 1+1 Hot Standby link inaccessible and therefore require an engineer to visit the site to perform the upgrade.

NOTE

Before upgrading the software, check that no alarms are outstanding for the units to be upgraded. See Managing alarms on page 7-15.

It is expected that upgrades will normally take place from an initial status of Primary to Primary, especially for an asymmetric coupler or for a protected antenna when the inactive unit has a lower capacity.

If the 1+1 Hot Standby link is operational, upgrade the units in the following order:

1. Disable local and remote protection switching. See Enabling and disabling fault protection on page 7-43.
2. If link planning indicates that the inactive units are able to operate a link of satisfactory quality, go to step 3. Otherwise, force a protection switch at one end of the wireless link, as described in Forcing protection switches on page 7-37, so that the link is operating between a primary and a secondary unit.
3. Upgrade software on the remote inactive CMU, then on the local inactive CMU.
4. Force a protection switch at both ends to inactive CMUs and check that the link is working.
5. Upgrade software on the remote (formerly active) CMU, then on the local (formerly active) CMU.
6. Test that the upgrade is successful as follows:

   If the coupler is symmetric, or if the coupler is asymmetric but the secondary units provide a good quality link, perform these tests:

   a. Force a local protection switch and check that the link is working.
   b. Force a protection switch at the other end of the wireless link to return to the initial configuration.

   If the couper is asymmetric, or if the antenna is protected and the inactive neighbor has a lower capacity:

   a. Force a combined protection switch and check that the link is working.

   Force a local end protection switch so that the optimum performing units are in use, that is, Primary to Primary.
7. Re-enable local and remote protection switching.

NOTE

After reboot of software on an operational 1+1 Hot Standby link which requires new RFU firmware, do not re-enable protection switching until after the inactive unit firmware upgrade has been completed. Otherwise, the RFU will reset after the firmware upgrade, potentially causing a protection switch.

Checking the recovery version

To confirm the recovery software version, select menu option **System, Software Upgrade** and note the Recovery Software Image attribute.

Using recovery mode

This section describes how the CMU enters recovery mode and how to recover the CMU.

For a general description of the recovery mode, see Recovery mode on page 1-62.

> **NOTE**
> When the CMU is in recovery mode, it cannot be recovered via a remote network connection. It can only be recovered from a PC that is directly connected to the Management port using the default IP address 169.254.1.1.

Entering recovery mode

When the CMU Modem LED (Table 5) blinks red, the CMU has entered recovery mode automatically. The CMU may enter recovery mode automatically in the following circumstances:

- When a checksum error occurs for the main application software image.
- When the Short Power Cycle for Recovery attribute is enabled (Table 232), the CMU is power cycled and the “off” period is between one and five seconds.

To enter recovery mode manually, proceed as follows:

1. Power off the CMU.
2. Press the CMU front panel Recovery button (Figure 4).
3. Keep the Recovery button pressed while powering on the CMU. Keep the Recovery button pressed for at least 20 seconds after powering on.
4. Wait until the CMU Modem LED blinks red, indicating that the CMU is in recovery mode.
5. Proceed with recovery options, as described below.

Selecting recovery option

Before starting this task, check that the CMU is in recovery mode. When the CMU Modem LED (Table 5) blinks red, the CMU is in recovery mode.

To select the CMU recovery option, proceed as follows:

1. Start the web browser.
2. Type IP address 169.254.1.1 into the address bar and press ENTER.

   The Recovery Mode Warning page is displayed (Figure 200).
3. Click anywhere on the Recovery Mode Warning page.

   The Recovery Options page is displayed (Figure 201).
4. Select the required recovery option and perform the recovery task (Table 262).

Figure 200 Recovery Mode Warning page

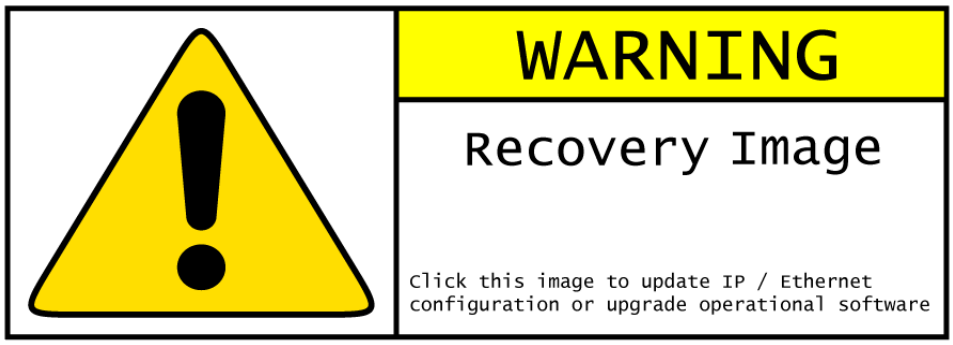


Figure 201 Recovery Options page

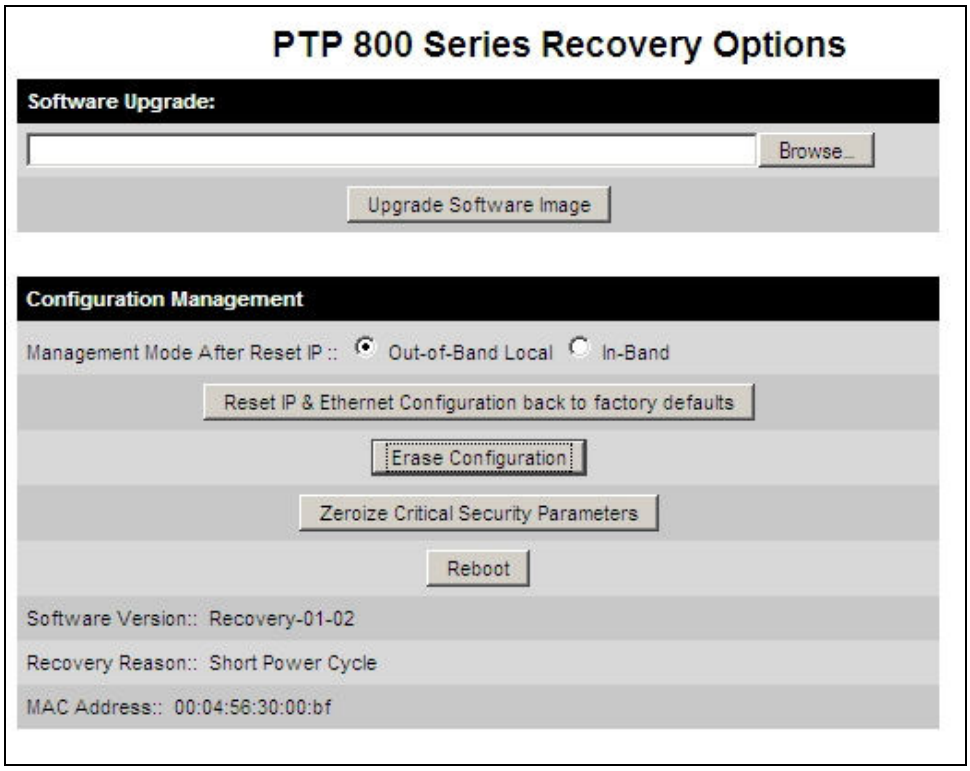


Table 262 Recovery options

Option	Recovery task
Upgrade Software Image	Upgrading software image on page 7-74.
Management Mode After Reset IP	This option selects the management mode that will be configured following reset of the IP and Ethernet configuration, or following erasure of all configuration data.
Reset IP & Ethernet Configuration back to factory defaults	Resetting IP and Ethernet configuration to factory defaults on page 7-75.
Erase Configuration	Erasing configuration on page 7-76.
Zeroize Critical Security Parameters	Zeroizing security parameters on page 7-76.
Reboot	This option is used to reboot the CMU after resetting configuration or parameters, as described in the above recovery tasks.

Upgrading software image

Perform this task when the CMU is in recovery mode. The purpose of this task is to replace a corrupt or unwanted software image. Before starting this task, check that the Recovery Options page is displayed (Figure 201).

To upgrade the software image in recovery mode, proceed as follows:

1. Select **Browse**. Navigate to the folder containing the required software image (PTP 800-nn-mm.dld2) and select **Open**.
2. If software corruption is suspected, select the software image that was installed when the CMU went into recovery mode. If an incorrect image has been loaded, select the correct software image.
3. Select **Upgrade Software Image**. The Software Upgrade Confirmation page is displayed (Figure 202).
4. Select **Program Software Image into Non-Volatile Memory**. The Progress Tracker page is displayed. On completion, the Software Upgrade Complete page is displayed (Figure 203).
5. Select **Reboot Wireless Unit**. The Reboot Confirmation dialog is displayed.
6. Select **OK**. The reboot progress message is displayed. On completion, the CMU restarts with the new software installed.

Figure 202 Recovery Software Upgrade confirmation page

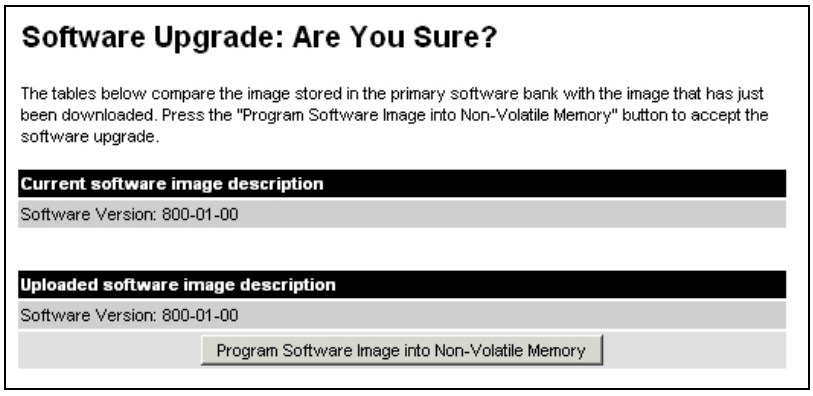

Software Upgrade: Are You Sure?
The tables below compare the image stored in the primary software bank with the image that has just been downloaded. Press the "Program Software Image into Non-Volatile Memory" button to accept the software upgrade.
Current software image description
Software Version: 800-01-00
Uploaded software image description
Software Version: 800-01-00
Program Software Image into Non-Volatile Memory

Figure 203 Recovery Software Upgrade complete page


Software Upgrade Complete
The software upgrade was completed Successfully. To complete the upgrade a system reboot is required. Please use the 'Reboot Wireless Unit' button below to reboot the unit.
Current software image description
Software Version: 800-01-00
Reboot Wireless Unit

Resetting IP and Ethernet configuration to factory defaults

Perform this task when the CMU is in recovery mode. The purpose of this task is to reset IP and Ethernet configuration back to factory defaults.

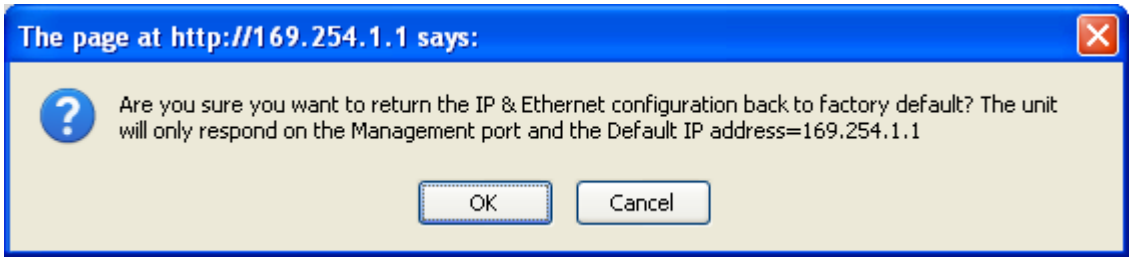
Before starting this task, check that the Recovery Options page is displayed (Figure 201).

To reset IP and Ethernet configuration parameters, proceed as follows:

1. Select **Reset IP & Ethernet Configuration back to factory defaults**. The Reset Configuration dialog is displayed (Figure 204).
2. Select **OK**. The Recovery Options page is redisplayed with a message indicating that the configuration has been reset.
3. Select **Reboot**. The Reboot Confirmation dialog is displayed.
4. Select **OK**. The reboot progress message is displayed. On completion, the CMU restarts.
5. To restore the IP and Ethernet configuration to meet the operator's requirements, see Task 2: Configuring IP and Ethernet interfaces on page 6-8.

> **NOTE**
> When the CMU is rebooted after selecting the recovery option **Reset IP & Ethernet Configuration back to factory defaults**, the IP address remains at its default setting of 169.254.1.1 and the CMU can only be accessed via a direct network connection from the PC to the management port.

Figure 204 Reset Configuration dialog


The page at http://169.254.1.1 says:
Are you sure you want to return the IP & Ethernet configuration back to factory default? The unit will only respond on the Management port and the Default IP address=169.254.1.1
OK
Cancel

Erasing configuration

Perform this task when the CMU is in recovery mode. The purpose of this task is to erase all changes that have been made to the configuration of the CMU and return it to its factory settings. This includes all changes made to the wireless, IP, Ethernet, license key, security, fault and performance parameters.

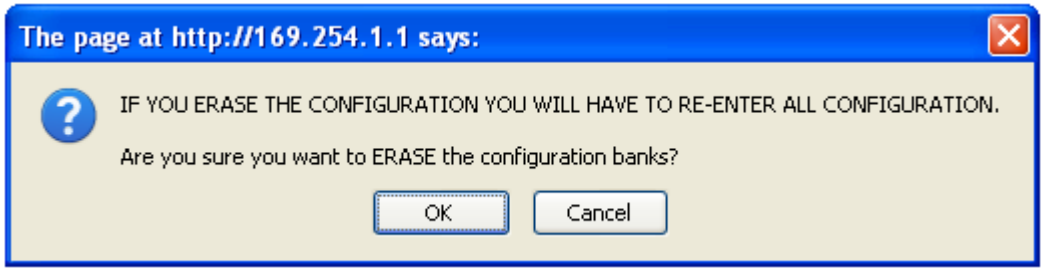
Before starting this task, check that the Recovery Options page is displayed (Figure 201).

To erase the entire configuration of the CMU, proceed as follows:

1. Select **Erase Configuration**. The Erase Configuration dialog is displayed (Figure 205).
2. Select **OK**. The Recovery Options page is redisplayed with a message indicating that the configuration has been erased.
3. Select **Reboot**. The Reboot Confirmation dialog is displayed.
4. Select **OK**. The reboot progress message is displayed. On completion, the CMU restarts.
5. Reconfigure the PTP 800 to meet the operator's requirements.

> **NOTE**
> When the CMU is rebooted after selecting the recovery option **Erase Configuration**, the IP address remains at its default setting of 169.254.1.1 and the CMU can only be accessed via a direct network connection from the PC to the management port.

Figure 205 Erase Configuration dialog


The page at http://169.254.1.1 says:
IF YOU ERASE THE CONFIGURATION YOU WILL HAVE TO RE-ENTER ALL CONFIGURATION.
Are you sure you want to ERASE the configuration banks?
OK
Cancel

Zeroizing security parameters

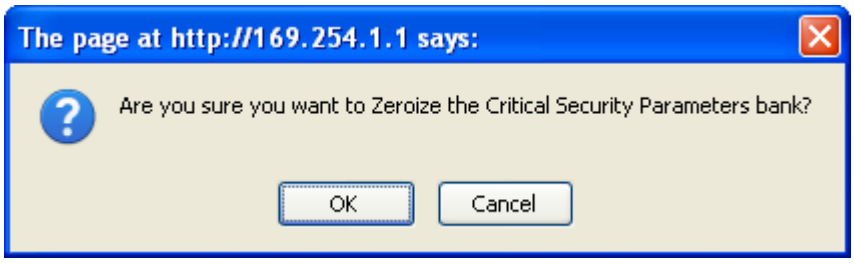
Perform this task when the CMU is in recovery mode. The purpose of this task is to zeroize the critical security parameters of the CMU.

Before starting this task, check that the Recovery Options page is displayed (Figure 201).

To erase the critical security parameters of the CMU, proceed as follows:

1. Select **Zeroize Critical Security Parameters**. The Zeroize Security Parameters dialog is displayed (Figure 206).
2. Select **OK**. The Recovery Options page is redisplayed with a message indicating that the security parameters have been zeroized.
3. Select **Reboot**. The Reboot Confirmation dialog is displayed.
4. Select **OK**. The reboot progress message is displayed. On completion, the CMU restarts.

Figure 206 Zeroize Security Parameters dialog



Downgrading PTP 800 software

To downgrade to an older version of PTP 800 software:

- Carefully record the existing configuration of the link
- Delete all configuration data as described in Erasing configuration on page 7-76
- Load the older software image as described in Upgrading software image on page 7-74.
- Re-install using the Installation Wizard and Configuration pages.

> **NOTE**
> Units with Recovery Image Software Recovery-04-00 cannot be downgraded to application software earlier than 800-04-00. See Checking the recovery version on page 7-70.

Chapter 8: Troubleshooting

This chapter describes how to identify and correct faults in a PTP 800 link.

The following topics are described in this chapter:

- Connecting to the web management interface on page 8-2: perform this task if any problems are encountered when connecting to the PTP 800 web interface.
- Installing the link on page 8-9: perform this task if any problems are experienced with a newly installed (or operational) wireless link.
- Testing protection switchover on page 8-13: perform this task if any problems are experienced with protection switchovers in a newly installed (or operational) 1+1 Hot Standby link.

Connecting to the web management interface

Perform this task if any problems are encountered when connecting to the PTP 800 web interface.

Check the CMU power indicator

The CMU power indicator shows the presence of the DC supply within the CMU.

Check the state of the CMU power indicator and take action as described in Table 263.

Table 263 CMU power indicator checks

CMU power indicator state	Likely cause and action
Green steady	Continue at Check the CMU status indicator on page 8-3.
Off	The DC supply may be absent or the CMU may be faulty. Continue at Check the DC supply to the CMU on page 8-2.

Check the DC supply to the CMU

Check the DC supply at the CMU using a suitable voltmeter and take action as described in Table 264.

Table 264 DC supply checks when CMU power indicator is off

DC supply state	Likely cause and action
Absent or less than –40.5 V	Check the AC supply, power converters, wiring, circuit breakers and fuses as appropriate.
Reversed polarity	The CMU has been damaged. Return the CMU to Cambium for repair.
Correct polarity and within the range –40.5 V to –60 V.	The CMU has an internal power supply fault. Return the CMU to Cambium for repair.

Check the CMU status indicator

The CMU status indicator shows if the CMU has a hardware fault, is booting, is operating in recovery or is operating in normal mode. Additionally, in normal mode it indicates if the wireless link is up or down.

Check the state of the CMU status indicator and take action as described in Table 265.

Table 265 CMU status indicator checks

CMU status indicator state	Likely cause and action
Green steady, green slow blink	The CMU is operating in normal (not recovery) mode. If the CMU has not yet been attached to a network, or if network is designed for out-of-band management, continue at Check the Management port Ethernet connection on page 8-4. If the network is designed for in-band management and the copper port is in use, continue at Check the copper Data port Ethernet connection on page 8-5. If the network is designed for in-band management and the fiber port is in use, continue at Check the fiber Data port Ethernet connection on page 8-6.
Orange steady	The CMU is booting. If the status indicator remains yellow steady for longer than 60 seconds, then continue at Using recovery mode on page 7-71, selecting the option to reload application software.
Red steady	The CMU is out of service. Continue at CMU out of service on page 8-3.
Red slow blink	The CMU is operating in recovery mode. Continue at Using recovery mode on page 7-71.
Off	If the CMU power indicator is illuminated and the status indicator is off, then the CMU has an internal power supply fault. Return the CMU to Cambium for repair.

CMU out of service

The out of service condition is shown by red steady illumination of the CMU status indicator. Continue at Using recovery mode on page 7-71, selecting the option to reload application software.

Check the Management port Ethernet connection

Check the state of the Management port indicators and take action as described in Table 266.

Table 266 Management port indicator checks

Management port indicator state	Likely cause and action
Yellow steady	The Ethernet link is up but is not carrying traffic. Continue at Check IP network connection on page 8-7.
Yellow blink	The Ethernet link is up and is carrying traffic. Continue at Check IP network connection on page 8-7.
Off	The Ethernet link is down. Continue at Management port indicator is off on page 8-4.

Management port indicator is off

If the Management port indicator is off, it means that the Ethernet link is down.

If the CMU Management port is connected to a management network, check the following:

- The associated network equipment (workstation, PC, router, switch etc.) is powered up and operating correctly.
- The Ethernet port in the associated equipment is enabled.
- The Ethernet cable between the CMU and the network equipment is connected and is not damaged. If possible, substitute a known good Ethernet cable.
- The Ethernet ports have compatible auto negotiation and duplex settings as described in Configuring the IP interface and management mode on page 6-10.

If the CMU Management port is connected directly to a PC, check the following:

- The Ethernet port in the PC is enabled.
- The Ethernet cable between the CMU and the PC is connected and is not damaged. If possible, substitute a known good Ethernet cable.
- The Ethernet ports have compatible auto negotiation and duplex settings as described in Configuring the IP interface and management mode on page 6-10.

If these steps fail to resolve the problem, continue at Using recovery mode on page 7-71, selecting the option to reset IP and Ethernet configuration.

Check the copper Data port Ethernet connection

Check the state of the copper Data port indicators and take action as described in Table 267.

Table 267 Copper Data port indicator checks

Copper Data port indicator state	Likely cause and action
Yellow steady, green steady	The Ethernet link is up but is not carrying traffic. Continue at Check IP network connection on page 8-7.
Yellow blink, green blink	The Ethernet link is up and is carrying traffic. Continue at Check IP network connection on page 8-7.
Off	The Ethernet link is down. Continue at Copper Data port indicator is off on page 8-5.

Copper Data port indicator is off

If the Copper Data port indicator is off, it means that the Ethernet link is down.

If the CMU copper data port is connected to a network, check the following:

- The associated network equipment (workstation, PC, router, switch etc.) is powered up and operating correctly.
- The Ethernet port in the associated equipment is enabled.
- The Ethernet cable between the CMU and the network equipment is connected and is not damaged. If possible, substitute a known good Ethernet cable.
- The Ethernet ports have compatible auto negotiation and duplex settings as described in Configuring the IP interface and management mode on page 6-10.

If the CMU Data port is connected directly to a PC, check the following:

- The Ethernet port in the PC is enabled.
- The Ethernet cable between the CMU and the PC is connected and is not damaged. If possible, substitute a known good Ethernet cable.
- The Ethernet ports have compatible auto negotiation and duplex settings as described in Configuring the IP interface and management mode on page 6-10.

If these steps fail to resolve the problem, continue at Using recovery mode on page 7-71, selecting the option to reset IP and Ethernet configuration.

Check the fiber Data port Ethernet connection

Check the state of the fiber Data port indicator and take action as described in Table 268.

Table 268 Fiber Data port indicator checks

Fiber Data port indicator state	Likely cause and action
Green steady	The Ethernet link is up but is not carrying traffic. Continue at Check IP network connection on page 8-7.
Green blink	The Ethernet link is up and is carrying traffic. Continue at Check IP network connection on page 8-7.
Off	The Ethernet link is down. Continue at Fiber Data port indicator is off on page 8-6.

Fiber Data port indicator is off

If the Fiber Data port indicator is off, it means that the Ethernet link is down. Check the following:

- The fiber adaptor is correctly inserted at the CMU.
- The fiber cable is correctly connected to the adaptor.
- The associated network equipment (router, switch etc.) is powered up and operating correctly.
- The fiber port in the associated equipment is enabled.
- The fiber cable between the CMU and the network equipment is connected and is not damaged. If possible, substitute a known good fiber cable.

If these steps fail to resolve the problem, continue at Entering recovery mode on page 7-71, selecting the option to reset IP and Ethernet configuration.

Check IP network connection

If the Management port indicators are illuminated (for a network using out-of-band management) or the Data port indicators are illuminated (for a network using in-band management) but the IP address of the CMU is unknown, continue at Entering recovery mode on page 7-71, selecting the option to reset IP and Ethernet configuration.

If the IP address of the CMU is known, send a sequence of ICMP Echo Request packets to the CMU management agent using the Ping program at the command line interface of the management PC or workstation.

If the CMU responds then the command line will appear similar to this:

```
C:\ping 169.254.1.1

Pinging 169.254.1.1 with 32 bytes of data:

Reply from 169.254.1.1: bytes=32 time=1ms TTL=64
Reply from 169.254.1.1: bytes=32 time<1ms TTL=64
Reply from 169.254.1.1: bytes=32 time<1ms TTL=64
Reply from 169.254.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 169.254.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1 ms, Average = 0ms
```

If the CMU fails to respond then the command line will appear similar to this:

```
C:\ping 169.254.1.1

Pinging 169.254.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 169.254.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Check the Ping response and take action as described in Table 269.

Table 269 Ping response checks

Ping response	Likely cause and action
Reply	The IP network is providing connectivity between the PC and CMU. Continue at Check browser settings on page 8-8.
Request timed out	There is no IP connectivity. Check network configuration including IP addresses, gateway address, subnet masks, VLAN membership in network equipment between the PC and the CMU. Check if the PC can reach other equipment in the same network. If these steps fail to resolve the problem, continue at Entering recovery mode on page 7-71, selecting the option to reset IP and Ethernet configuration.

Check browser settings

If there is IP connectivity between the CMU and the management PC or workstation, but web-pages cannot be displayed, check that browser settings are appropriate for the PTP 800 web interface.

Installing the link

Perform this task if any problems are experienced with a newly installed (or operational) wireless link.

Connect to the web management interface

See Connecting to the web management interface on page 8-2.

Check RFU status

RFU status is indicated by the RFU Status attribute in the Status screen of the web interface.

Check the RFU Status attribute and take action as described in Table 270.

Table 270 RFU status checks

RFU Status attribute	Likely cause and action
OK	The RFU is available for use. Continue at Transmitter status on page 8-10.
Download In Progress	The CMU is downloading updated firmware to the RFU. Wait for the download to complete.
No Response	The RFU is not responding to management messages from the CMU. Check connections and continue at Testing the ODU and IF cable on page 5-60.
Power Supply Fault	The CMU cannot power the RFU. Check connections and continue at Testing the ODU and IF cable on page 5-60.
RFU Fault	The RFU is reporting a fault condition.
Incompatible Device Incompatible Firmware Version	The RFU firmware is not compatible with the CMU. Replace the RFU.

Transmitter status

Transmitter status is indicated by the Transmitter Status attribute in the Status Screen of the web interface and in Step 6: Antenna Alignment of the Installation Wizard.

The transmitter is muted by default. The transmitter is enabled automatically during installation in Step 6: Antenna Alignment of the Installation Wizard. The transmitter may additionally be enabled or muted using the Configuration page of the web interface.

Go to the Status page, or use the Installation Wizard and navigate to Step 6: Antenna Alignment. Check the Transmitter Status attribute and take action as described in Table 271.

Table 271 Transmitter Status checks

Transmitter Status attribute	Action
Transmitting	Continue at Antenna alignment on page 8-10.
Muted – By User	The Antenna Alignment step of the Install Wizard has not been completed successfully, or the transmitter has been muted using the Mute Transmitter button on the Configuration Page. Restart the Installation Wizard.
Muted – RFU Configuring	Transmission is disabled while the RFU configuration is changing. This status will normally exist for no more than a few seconds.
Muted – RFU Fault	There is a fault in the RFU. Use the Home page to review the RFU alarms.
Muted – Configuration Error	The RFU is not compatible with the configured radio license. Restart the Installation Wizard.
Muted - Due to standby	The CMU is the inactive unit of a 1+1 protected end.

Antenna alignment

Repeat the Antenna Alignment procedure as described Step 6: Aligning antennas on page 6-100.

Check the receive power from the RSSI connector of the RFU, or from the Receive Power attribute in Step 6: Antenna Alignment.

If the receive power level is very small or cannot be measured, continue at Check transmit and receive frequencies on page 8-11.

If the receive power is close to the predicted power for the link then continue at Check link status on page 8-11.

Check transmit and receive frequencies

Check that the transmit frequency at the near end of the link is exactly equal to the receive frequency at the remote end of the link.

Check that the receive frequency at the near end of the link is exactly equal to the transmit frequency at the remote end of the link.

If this fails to resolve the problem, continue at Check waveguide and antennas

Check waveguide and antennas

Check the antennas, waveguides, RMKs and couplers for defects and incorrect assembly.

If this fails to resolve the problem replace the near end RFU and, if necessary, replace the remote RFU.

Check link status

Link status is indicated by the Link Status attribute on the System status page of the web interface.

If the receive signal power is close to the predicted value, check the Link Status attribute and take action as described in Table 272.

Table 272 Link Status checks

Link Status attribute	Action
Searching	Check that the same channel bandwidth is configured for both ends of the link
Acquiring Registering	Check the System Summary for a Link Name mismatch alarm. If present, correct Link Name so that it is identical at both ends of the link.

Check IRFU status LEDs

Table 273 IRFU LED status checks

Label	LED	Condition	Remedy / action
PWR	Green	Power supply is ON	Do nothing
	Off	Power supply is OFF	Push PWR button ON
ALM	Green	Indicates no hardware failure	Do nothing
	Yellow	Flashing, indicates fans failure or degradation	Verify fan wire leads, clean, reconnect or replace the faulty fan assembly when necessary; refer to Replacing a fan assembly on page 5-103.
		Flashing, RF loopback activated	Normal, do nothing
		Temperature sensor in the PA module exceeds threshold	Check if the Fan alarm is On, or if the ambient temperature exceeds +50 °C. If not, and the sensor temperature remains higher than the threshold (75 °C) for a long time, refer to Replacing a transceiver on page 5-97.
	Red	Flashing, indicates hardware failure, “Replace Me”	Replace the Transceiver, refer to Replacing a transceiver on page 5-97.

Testing protection switchover

Perform this task if any problems are experienced with protection switchovers in a newly installed (or operational) 1+1 Hot Standby link.

Check protection interface status

Check Protected Interface Status in the System Summary page as described in Table 274.

In a 1+1 Hot Standby configuration, information is shared between neighbor CMUs over the protection interface. The Protection Interface Status attribute reports whether the neighbor CMU is successfully responding, physically disconnected or whether it is physically connected but not responding, for example powered down.

Table 274 Protected Interface Status values and actions

Value	Meaning	Action
OK	The CMU has detected that the neighboring CMU is responding.	Check that protection switching is enabled, the status of the wireless link and consider forcing a protection switchover.
Neighbor not connected	The neighbor CMU is not physically present.	Check that the protection interface is correctly connected.
Neighbor not responding	The neighbor CMU is not responding	Check the status of the second CMU.

Check that protection switching is enabled

Check the Protected Link page as described in Managing 1+1 Hot Standby links on page 7-33.

If protection switching is disabled for this end of the wireless link, re-enable it, see Enabling and disabling fault protection on page 7-43.

If the Protection Link screen indicates that there are alarms for this unit then follow the trouble shooting guide for the alarms indicated.

Check the status of the wireless interface

Check the status of the wireless interface, see Check link status on page 8-11.

> **NOTE**
> If the wireless link quality has been affected by adverse weather it is likely that the secondary unit will not be able to provide a service either, particularly if an asymmetric coupler has been used or the secondary unit is providing antenna protection with a less powerful antenna.

Check the link protection cable

Check the link protection cable is connected as described in Preparing network connections (1+1 Hot Standby) on page 5-89.

Force a protection switchover

Consider manually initiating a protection switchover as described in Forcing protection switches on page 7-37, provided the link planning indicates that the units have the capability of operating a link of satisfactory quality.

This particularly applies where asymmetric couplers have been used, or a secondary antenna of lower power.

Check the configuration of the active and inactive units

Check that the active and inactive units have a compatible configuration.

They must be configured to have:

- The same link parameters;
- The same radio licence parameters;
- The same radio parameters;
- The same encryption parameters;
- The same management and protection options;
- The same data connectivity parameters

They must be configured to have different IP addresses and different primary/secondary attributes.

Glossary

Term	Definition
ACM	Adaptive Coding and Modulation
AES	Advanced Encryption Standard
ATPC	Automatic Transmitter Power Control
BU	Branching Unit of IRFU
CAVP	Cryptographic Algorithm Validation Program
CEPT	European Conference of Postal and Telecommunications Administrations
CHAP	Challenge-Handshake Authentication Protocol
CIR	Committed Information Rate
CMU	Compact Modem Unit
CSP	Critical Security Parameter
DES	Data Encryption Standard
DSCP	Differentiated Services Code Point
EAPS	Ethernet Automatic Protection Switching
EIRP	Equivalent Isotropic Radiated Power
EMC	Electromagnetic compatibility
EMD	Electromagnetic discharge
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FEC	Forward Error Correction
FIPS	Federal Information Processing Standard
GARP	Generic Attribute Registration Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS/TLS	HTTP over Transport Layer Security
IC	Industry Canada
ICMP	Internet Control Message Protocol

Term	Definition
ID	Identity
IEEE	Institute of Electrical and Electronic Engineers
IF	Intermediate Frequency
IP	Internet Protocol
IRFU	Indoor Radio Frequency Unit
ITU	International Telecommunications Union
LAN	Local Area Network
LDPC	Low Density Parity Check
LOS	Line-of-Sight (clear line-of-sight, and Fresnel zone is clear)
LPU	Lightning Protection Unit
LTE	3GPP Long Term Evolution
MAC	Medium Access Control Layer
MD5	Message Digest Algorithm
MHSB	Monitored Hot Standby
MIB	Management Information Base
MRP	Multiple Registration Protocol
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
ODU	Outdoor Unit
OMK	Orthogonal Mounting Kit
PC	IBM Compatible Personal Computer
PING	ICMP Echo Request
PTP	Point-to-Point
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RMK	Remote Mounting Kit
RFU	Radio Frequency Unit (ODU or IRFU)

Term	Definition
RMS	Rack Mounting Space. 1 RMS is 44.45 mm (1.75 inch) high.
RF	Radio Frequency
RSL	Receive Signal Level
RSSI	Received Signal Strength Indication
Rx SD	Receive Spatial Diversity
SD	Spatial Diversity
SELV	Safety Extra Low Voltage
SFP	Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPID	Tag Protocol Identifier
URL	Universal Resource Location
UV	Ultraviolet
VID	VLAN Identifier
VLAN	Virtual Local Area Network
VSWR	Voltage Standing Wave Ratio